S. HRG. 107–1150

S. 2201, ONLINE PERSONAL PRIVACY ACT

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

APRIL 25, 2002

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

91–368 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii	JOHN MCCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAUX, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBACK, Kansas
BARBARA BOXER, California	GORDON SMITH, Oregon
JOHN EDWARDS, North Carolina	PETER G. FITZGERALD, Illinois
JEAN CARNAHAN, Missouri	JOHN ENSIGN, Nevada
BILL NELSON, Florida	GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*
JEANNE BUMPUS, *Republican Staff Director and General Counsel*

CONTENTS

S. 2201, ONLINE PERSONAL PRIVACY ACT

THURSDAY, APRIL 25, 2002,

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:15 a.m. in room SR–253, Russell Senate Office Building, Hon. Ernest F. Hollings, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. ERNEST F. HOLLINGS, U.S. SENATOR FROM SOUTH CAROLINA

The CHAIRMAN. The Committee will come to order. What we have, of course, is our online privacy bill before the Committee, and we have an actual bipartisan bill. The interesting thing is that—and I will put my full statement in the record, but we have got 14 different laws and regulations offering different levels of notice, choice, access and everything else, we have got the Cable Act, the Junk Fax Act, the telemarketing privacy, the video privacy—I comment on that because you would think, in trying to propose privacy for the Internet, that we are doing something real radical—not at all.

In fact, you look at the European practice, we have got some 135 blue chip American corporations that have joined in their particular opt-in online privacy provisions, which in a way in a couple of regards are even a little more stringent than ours, but be that as it may, the bipartisan bill sets a uniform Federal standard for the protection of online personal information, and the five core principles are consent, notice, access, security, enforcement.

I want to particularly, of the nine cosponsors, thank Senators Inouye, Rockefeller, Breaux and Cleland, who started with us—this has been a sort of a 2–1/2 year exercise, and Senators Kerry, Stevens, and Burns now, who worked with us the past 7 months to craft a bill that takes care of the concerns, not just of the consumers but, of course, the industry itself.

We do not want to do anything to stultify—in fact, it is this Senator's view that in providing privacy provisions we are actually establishing trust and confidence in the Internet and therefore encouraging and propagating better and increased use. It has a provision for strong preemption. That is the certainty needed to resolve conflicting State standards. It has an opt-in protection for the sensitive personal information such as financial, health, ethnicity, religious preference, sexual orientation. It has opt-out protection for nonsensitive personal information like marketplace purchases. It has reasonable access, reasonable security and a sensible enforce-

ment by the FTC and the State Attorneys General, of course with the private right of action.

When we look at the Federal Trade Commission they have had some 5 years of studies, hearings, meetings with the industry off and on, and the last Federal Trade Commission recommended, in futility, that we legislate, because they could not get an agreed approach, but you can see how the Federal Trade were treated. Eli Lilly exposed 700 Prozac patients and got just a slap on the wrist, so we have it in there as a private right of action with jurisdiction in the Federal court and a showing of actual harm.

My full statement is in the record. Let me yield. Senator McCain.

[The prepared statement of The Chairman follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS, U.S. SENATOR FROM SOUTH CAROLINA

Today the Commerce Committee will examine S. 2201, the Online Personal Privacy Act of 2002—a bipartisan bill that is sponsored by 10 Senators on this Committee. We plan to report a bill in May, and that makes today's hearing exceedingly timely. It's past time for action on this issue, today will mark the 6th hearing on internet privacy in the last two Congresses. American consumers deserve better privacy protection on the Internet. We intend to give it to them.

I am pleased to be joined in my efforts by nine cosponsors on this Committee. We have those who were with me from the beginning—Senators Inouye, Rockefeller, Breaux, and Cleland. And we have additional support, from Senators Kerry, Nelson, Carnahan, Stevens and Burns. I particularly want to commend Senators Kerry, Stevens, and Burns, who have worked with me over the past seven months to craft the sensible, balanced approach that we introduced last week.

Let me articulate the principles that allowed us to achieve strong bipartisan support for our legislation—

- Strong preemption (to give business the certainty it needs in the face of conflicting state standards)
- Opt-in protection for sensitive personal information (like your financial and health information, your ethnicity, religious preferences, or sexual orientation)
- Opt-out protection for non-sensitive personal information (like your name and address, and marketplace purchases)
- Reasonable access
- Reasonable security
- Sensible enforcement by the ftc and the state ags, with the limited exception of violations involving sensitive information, which permit a right of action in federal court, premised on a showing of actual harm.

Why do we need legislation? Businesses keep confounding consumers with unclear privacy policies that state, "your privacy is important to us," but subsequently outline exceptions crafted to allow almost any use of personal information. Other Web sites don't post privacy policies, safe in the knowledge that they face no legal jeopardy under current law for selling your information.

Some have argued that Americans' concerns about privacy no longer exist after September 11th. But poll after poll consistently demonstrates the American people want companies they patronize to seek their permission prior to using their personal information for commercial profit. As recently as February, a Harris survey found that 63% of Americans want internet privacy legislation.

At the same time, advances in technology have provided the tools to seamlessly compile and enhance highly detailed personal profiles and histories of Internet users. Cookies and web bugs, and who knows what other technologies, all enable the surreptitious collection of individuals' personal information, including every click of their computer mouse, online.

Moreover, severe privacy breaches continue without consequence. Last year, Eli Lilly disclosed a list of hundreds of customers suffering from depression, bulimia, and obsessive compulsive disorder. Eli Lilly's response? An apology, and a promise it won't happen again. But an apology and a promise is not enough for those patients whose medical history was divulged publicly.

Sensible privacy legislation like S. 2201 will stop this, promote consumer confidence, and bolster online commerce. A recent Forrester study reports that online businesses lost $15 billion due to consumer privacy concerns. Those numbers are significant in light of the economic downturn and its exaggerated impact on the high tech internet sector. Good privacy means good business and the internet economy could use a dose of that right now.

The shame is that it has taken us this long to get here. It has been nearly two years since the FTC recommendation for Internet privacy legislation, which was reached after five years of diligent study. This recommendation was particularly credible in light of the FTC's record of extensive analysis and its two prior recommendations to allow self-regulation a chance to work.

We will hear from our opponents today that it is unfair to regulate online only. But this argument is nothing more than a straw man designed to kill internet privacy legislation. Does anyone remember a similar argument when we passed the children's privacy legislation? Were children's web sites complaining that we were regulating them differently from Toys-R-Us? Of course not. The internet industry supported that legislation. This Committee stands ready to pass similar legislation for all users. Lets start there and then we'll see about the entire marketplace.

Others will complain that our bill is premature—that we need to give the Gramm-Leach-Bliley financial privacy rules a chance to work, before we alter them for the Internet. Well—we've seen those rules, and they don't work.

Americans have been receiving billions of notices in the mail telling them they can opt-out of the sharing of their personal financial information by financial institutions. These notices make a mockery of the claim that notice and opt-out provides sufficient protection for sensitive information. In many cases, the notices are internally inconsistent and outright deceptive.

We need to bring transparency and consistency to privacy protection on the internet by building on the many existing statutes that protect privacy for telephone customers, cable subscribers, video renters, credit card customers, and children on the internet. All Internet users deserve similar protection.

Some forward thinking companies know this. Microsoft, Intel, Hewlett-Packard, Expedia, and Earthlink provide opt-in right now. 185 U.S. companies, Including, Microsoft, Intel, Hewlett-Packard, and one of the largest data collection companies, Axciom, have signed on to the EU Safe Harbor, which requires notice, opt-in for sensitive information, access and security. Why should European citizens be granted more protection than Americans?

Finally, I want to note that the following high tech trade associations have called for privacy legislation that preempts state law, requires notice and an opportunity to opt-out (and sometimes, even opt-in): the Information Technology Industries Association; the American Electronics Association; the Computer Systems Policy Project; and the Computer Technology Industry Association. Many of the members of these associations actually provide better privacy protection themselves, voluntarily.

Despite the good intentions of these companies, unless we take action to establish common-sense protections that will deter bad actors, consumer fears will continue to stifle use of the internet as a trusted commercial medium.

I look forward to our witness testimony, and the remarks of my distinguished former chairman, Senator McCain.

STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

Senator MCCAIN. Thank you, Mr. Chairman, and I want to thank you for holding this hearing today on the topic of online privacy and your recently introduced bill. I want to thank you for your continued work on this important subject. It is clear that privacy continues to concern many Americans who use the Internet. In a recent Harris interactive poll a majority of the respondents once again voiced their concerns over the use of their personal information online.

In past hearings, this Committee has closely examined several issues with respect to online privacy legislation. We considered whether each of the four fair information principles, notice, choice, access, and security, should be mandated for online companies and, if so, how. We also addressed the questions of enforcement and pre-

emption of State law. The Chairman's bill includes each of these elements and offers a solution that seeks compromise on some of the differences we have explored in prior hearings.

Differences remain, however, particularly with respect to the private rights of action that this legislation creates, as well as the bill's coverage of access and security. There are, on an even broader level, very significant practical challenges we need to consider with respect to how or if this legislation can be implemented.

One challenge we face is the treatment of personally identifiable information that is collected from both online and offline sources, and then merged together in a single consumer data file. Many companies and institutions today operate in both the online and offline world. We see examples of this everywhere. The retail chain, Toys-R-Us, allows customers to shop for the same toys online at Amazon that they can buy in their stores and shopping centers. Many local banks have web sites that allow account holders to check balances, transfer funds between accounts, and write checks to pay their bills online.

These businesses must collect and use personal information in both settings in order to provide their goods and services, and sometimes that information must be combined into one customer file. What happens to that combined information if we attempt to legislate for the online world without considering its collection or use in the offline one? Would the same types of notices be applied, even ones designed with the Internet in mind?

As these two worlds merge, we must face the practical reality that restrictions intended for the online world may have unintended but significant impact on accepted business practices in the offline world.

The second challenge is that Congress passed over 30 Federal laws that already protect the privacy of individuals. We have to be certain to carefully consider the effect of this bill on these existing laws, particularly if its enactment would create ambiguous or conflicting requirements for business and greater confusion for consumers.

I would also like to introduce two items into the record today that I believe are essential to our consideration of this legislation. The first are the letters of the Chairman and commissioners of the Federal Trade Commission that I received yesterday afternoon, a second is the 2001 survey of online privacy practices released by the Progress and Freedom Foundation in March, which duplicated the methodology used by the FTC in its 2000 report.

The FTC has spent a considerable amount of time and resources addressing the issue of online privacy. After S. 2201 was introduced, I wrote a letter to each of the commissioners asking whether they believed legislation was needed and, if so, what it should contain. I also asked for their comments on the principle features of the legislation. Despite the short amount of time they had to spend, each commissioner did, and I thank them for their efforts. In summary, two of the five commissioners believe that legislation is needed at this time and are supportive of the bill. The other three commissioners, including the Chairman, expressed strong reservations about the workability of the provisions of S. 2201, and the need for

legislation in light of existing privacy law, increased FTC enforcement, and industry efforts to improve protections.

I want to thank the witnesses for being with us today, and I will be interested in hearing their views on the legislation. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Senator Burns.

STATEMENT OF HON. CONRAD BURNS,
U.S. SENATOR FROM MONTANA

Senator BURNS. Thank you, Mr. Chairman. Thanks for holding this hearing today as we wrestle with this problem of privacy in the Internet world. As more and more of our daily activities move online, it is no surprise that privacy is the number one concern among Internet users. I should add that privacy or, rather, the lack of it, is also the top reason why nonusers have not yet ventured into the Internet.

The reason for these well-justified concerns are clear. Americans have no safety net on privacy online. In fact, ever more sophisticated technologies are being developed to collect nearly limitless information on individuals without their knowledge. Privacy is not just an individual rights concern, however. Online privacy is central to the future of the economic well-being of the Internet. The rate of growth of e-commerce is clearly being slowed by consumers' rising and legitimate fears about privacy intrusion. Several studies pointed out that the privacy reason preventing more people from making purchases online is the lack of privacy.

While the Internet has exhibited massive growth, currently less than one percent of all consumer retail spending is done online. In short, e-commerce still has a huge upside potential, but that potential will never be fulfilled without the basic assurances of consumer privacy. To address these concerns, early in the 106th Congress, Senator Wyden and I introduced an Online Privacy Protection Act which was based on our shared view that while self-regulation should be encouraged, we need to also provide a strong enforcement mechanism to punish the bad actors.

I remain convinced that the comprehensive private legislation is necessary to protect consumers, which is why I am the original cosponsor of the bill the Committee is considering today, the Online Personal Privacy Act. The fact that the bipartisan bill was introduced last week with 10 cosponsors on the Committee shows a tremendous support for online privacy that exists on this Committee. The current bill is much improved from the previous versions, and, while it is not perfect by any means, I view it as a reasonable compromise between the opt-out approach, which I favored previously, and the opt-in approach which the Chairman's original bill incorporated.

I believe one of the strongest sections of the bill the Committee is considering today is its clear-cut preemption language. In response to the rising call for consumer privacy protection, the Internet risks being subject to a crazy quilt of conflicting regulations on a State-by-State basis. Already, for instance, the State of Minnesota has passed a comprehensive online privacy bill out of its legislature, and California is moving along a similar track. An online privacy law is already on the books in Vermont, which requires an

opt-in by consumers before individuals' financial or medical information can be shared with third parties.

While the impulse behind these efforts is understandable, companies need regulatory certainty in order to do business efficiently. Clearly, strong Federal preemption is needed and is provided in S. 2201.

The robust security requirement is also a very positive aspect of the current bill. The bill simply requires web sites to maintain a reasonable procedure necessary to protect security, confidentiality, and integrity of personally identifiable information. In today's era of hacker intrusion and identity theft, I view this section as absolutely essential to protect consumers.

I would like to touch on the idea offered by many who oppose privacy legislation that simply posting a privacy policy is the same as actually ensuring privacy for consumers. While I view the increasing trend toward posting privacy policies as a positive development, the fact remains that many of these policies are frustrating exercises in legalese. It becomes obvious from weeding through the examples of these policies that most were designed with the goal of protecting the companies, rather than informing and empowering the consumers.

A perfect example of the potential consequences of the legalistic approach toward privacy policies occurred earlier this month, when millions of consumers downloaded a file-swapping program called Kazaa. Only later did consumers realize that they had agreed to install software that could help turn their computers into nodes on a network controlled by a third company called Brilliant Entertainment, while the company's privacy policy ran over 4,000 words, which explains why most consumers simply clicked on the "I agree" button.

The concern surrounding these types of abuse led to the requirement in previous bills, on Senator Wyden's and my bill before, and S. 2201, that Privacy policies must be clear, and they must be conspicuous.

I look forward to working with the Chairman and my colleagues on the Committee on this critical issue. I also look forward to the testimony today, and I appreciate it, and thank the witnesses for coming today, and I thank the Chairman.

The CHAIRMAN. Thank you. Senator Allen.

STATEMENT OF HON. GEORGE ALLEN, U.S. SENATOR FROM VIRGINIA

Senator ALLEN. Thank you, Mr. Chairman, for holding this hearing. I have read and look forward to working with our witnesses, and thank you all for being here.

I think we all can agree that individual people have a significant interest in personal information and an interest in determining how that information is used. Now, throughout this debate, Mr. Chairman, and for those who are in the Committee room here, I have been guided by two principles.

First, I think we ought to empower individual consumers to make sure that they have the information necessary to make a reasonable decision and choice on their own. Second, I think we need

to encourage to the greatest extent possible market-driven regulation. Many of those market forces already exist.

Now, I want to associate myself, Mr. Chairman, with the sentiments expressed by Senator McCain, and I will not repeat many of the points he made, but I do want to touch on them. In this regard, I have concerns that this Committee may be proceeding with legislation prematurely that is unnecessarily burdensome and discriminatory to the online world. I do not think we should discriminate in the treatment of personally identifiable information with regard to the medium through which the information is collected. Why should a consumer's privacy concern regarding information-sharing only accommodate or apply to those consumers who have access to the Internet?

Second, and further, there are at least 23 current Federal laws addressing information-sharing and privacy rights. I understand that consumers have specific and legitimate concerns about his or her health and financial information privacy. In addition, whether online or offline, the Gramm-Leach-Bliley Act of 1999, and the Health Insurance Portability and Accountability Act of 1996 already address many of those specific concerns. I would encourage enforcement of our existing laws before we attempt to craft new laws.

Third, the Progress and Freedom Foundation released a report on online privacy, a report on the information practices and policies of commercial web sites. Some of the more interesting findings were that commercial web sites are collecting less personally identifiable information than they were 2 years ago. They also pointed out that fewer web sites are using third party cookies to track web surfing behavior.

Of the most popular web sites, showing the reaction of the private sector, the sites that receive the most traffic, the use of third party cookies fell from 78 percent to 48 percent, and also the privacy notices—and Senator Burns noted this—are more prevalent and more prominent and more complete.

Ninety-nine percent of the 85 busiest web sites have privacy policies that are more comprehensive, in other words, stating how they handle the consumer information, and more accessible from the site's front page.

Now, the one rational jurisdictional reason for this legislation and one that I, too, support, and I think is the most important part, has to do with the jurisdiction, the Federal jurisdiction in this, in that it does deal with interstate commerce. The reason the Senate should consider any privacy legislation is to establish a uniform national standard. To have a patchwork of liabilities and rules governed by the States would make it extremely difficult for any business to comply with 50 potentially conflicting privacy laws and regulations, thus arguably affecting interstate commerce.

I do want to get into some of the details of how much—and we do need to have a strong preemption. Some States, Mr. Chairman, and others are considering enacting privacy laws under the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, and how will these privacy laws be preempted under this legislation, and if we enact a new law I think we ought

to make certain that the strongest, most effective preemption language is included.

I would finally say that the treatment in here of affiliated companies as third parties can be seriously troublesome to diversified companies with diversified corporate structures. Many companies consist of dozens of different corporate structures, all of which may share a common customer data base. If a user's consent is required to share personally sensitive, personally identifiable information, even amongst controlled and affiliated subsidiaries, then many larger companies are going to be automatically potentially out of compliance, and just by the very nature of how data management infrastructures are built.

So I look forward to working to the extent we can, and I hope we can in a bipartisan fashion with our Committee Members in an approach that informs and empowers individual choice, but also trust the private sector to continue its good work in the market, and I believe that that approach means that we ought to move very cautiously.

I would finally state, Mr. Chairman, let us not create any more government-imposed restrictions that create more problems than they solve.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Senator Wyden.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you, Mr. Chairman. I want to start, Mr. Chairman, by commending you, because I think a lot of progress has been made in the last year on this issue. As all of us will recall a year ago, this Committee was to a great extent deadlocked over some arcane matters, particularly this opt-out and opt-in issue. You have produced a hybrid kind of approach that I think makes a lot of sense, and I am planning to work very closely with you in the days ahead so that we can report this legislation.

There is an important challenge today, because I do not think this country can afford an EXXON VALDEZ of privacy. We have already seen some very serious problems. It was not very long ago when the Eli Lilly Company unintentionally disseminated the e-mail addresses of more than 600 people taking Prozac, and I would just say, particularly to people in industry, if there is an EXXON VALDEZ of privacy, it will not be possible to get the kind of preemption protection that is envisaged in this legislation.

If there are those kinds of calamitous events, every State in this country is going to go off and essentially do their own thing, and at that point the horse will be out of the barn, and it will not be possible to get preemption protection, as many in industry are seeking.

Now, there are a number of concerns that I have at this point. I do want to make sure that with respect to the notice provision that there is a short, understandable notice provision, something that consumers can become familiar with in the years ahead.

I also think it is important to explore ideas for safe harbor provisions so that the many companies in this country that are acting responsibly will have a clear path of certainty and safety under the

legislation that Congress may pass, but there is no question in my mind important progress has been made in the last year, and I look forward to working with you, Mr. Chairman and Senator McCain and others to report this legislation.

The CHAIRMAN. Thank you. Senator Stevens.

STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

Senator STEVENS. Thanks very much, Mr. Chairman. I do not have a written statement, but I would say that I agree with Senator McCain about the offline concept, and I think we probably should be willing, those of us who sponsor this legislation, to listen to some of those concerns.

Also, I have some concerns that I have expressed to you about the right of private action, and I think there ought to be some limitation on that. We ought to rely on the agencies first and then rely on private action only when it is necessary to raise the issues in the courts.

And Senator McCain, I do not know if you know it, some of the commissioners sent us copies of the letters they wrote back to you, others did not. If you would share all of them with us, I think it would be good for the record to know what the commissioners are thinking about this. I do think, as Senator Allen said, we have a job to do now, and it is time that we got this done, and I think we should not be afraid of broadening this legislation.

Thank you very much.

The CHAIRMAN. Very good. Senator Cleland.

Senator MCCAIN. Mr. Chairman, I would ask the letters be included in the record.

The CHAIRMAN. Those letters will be included.

[The information referred to follows:]

FEDERAL TRADE COMMISSION
Washington, DC, April 24, 2002

Hon. JOHN MCCAIN,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Senator McCain:

Thank you for your letter of April 19, 2002, requesting my views on S. 2201, the Online Personal Privacy Act.

Personal privacy issues are a key priority at the Commission. Because a variety of practices can have negative consequences, consumer concerns about privacy are strong and justified. Avoiding these consequences requires a strong law enforcement presence, and we have increased by 50 percent FTC resources targeted to addressing privacy problems. Our agenda includes:

- A proposed rulemaking to establish a national, do not call registry;
- Greater efforts to enforce both online and offline privacy promises;
- Beefed up enforcement against deceptive spam;
- A new emphasis on assuring information security;
- Putting a stop to pretexting;
- Increased enforcement of the Children's Online Privacy Protection Act; and
- New initiatives to both help victims of I.D. theft and assist criminal prosecution of this crime.

The concerns about privacy that motivate our enforcement agenda have led others, including many members of Congress, to propose new laws, such as S. 2201, the Online Personal Privacy Act. There are potential benefits from general privacy

legislation. If such legislation could establish a clear set of workable rules about how personal information is used, then it might increase consumer confidence in the Internet. Moreover, federal legislation could help ensure consistent regulation of privacy practices across the 50 states. Although we should consider carefully alternative methods to protect consumer privacy and to reduce the potential for misuse of consumers' information, enactment of this type of general legislation is currently unwarranted. [1]

Five points underscore my concern about general, online privacy legislation:

1. Drafting workable legislative and regulatory standards is extraordinarily difficult.

The recently-enacted Gramm-Leach-Bliley Act ("GLB"), which applies only to financial institutions, required the multiple mailings of over a billion privacy notices to consumers with little current evidence of benefit. [2] Our experience with GLB privacy notices should give one great pause about whether we know enough to implement effectively broad-based legislation, even if it was limited to notices.

Unlike GLB, the proposed legislation deals with a wide variety of very different businesses, ranging from the websites of local retailers whose sales cross state lines to the largest Internet service providers in the world. Thus, implementation of its notice requirement will likely be even more complicated.

Moreover, the legislation adds requirements for access not found in GLB. The recommendations of the FTC's Advisory Committee on Online Access and Security make clear that no consensus exists about how to implement this principle on a broad scale. [3] Perhaps reflecting these same concerns, S. 2201 grants the FTC broad rulemaking authority. The only legislative guidance is the requirement that the procedures be reasonable. The statute is silent, for example, on how to balance the benefits of convenient customer access to their information with the inherent risks to security that greater access would create. The FTC has no answer to this conundrum. We do not know how to draft a workable rule to assure that consumers' privacy is not put at risk through unauthorized access.

The inherent complexity of general privacy legislation raises many difficulties even with provisions that are conceptually attractive in the abstract. For example, the proposed legislation imposes different requirements on businesses based on whether they collect "sensitive" or "nonsensitive" personal information. Although this may be a conceptually sound approach, we have no practical experience in implementing it, and attempting to draw such distinctions appears fraught with difficulty, both in drafting regulations and assuring business compliance. Under the statute, for example, the fact that I am a Republican is considered sensitive, but a list of books I buy and websites I visit are not.

Similarly, the broad state preemption provision would provide highly desirable national uniformity. Questions about the scope of preemption would inevitably arise, however. How would the preemption provision affect, for example, state laws on the confidentiality of attorney/client communications for attorneys using websites to increase their efficiency in dealing with their clients? Moreover, what are the implications for state common law invasion of privacy torts when the invasion of privacy occurs online?

Another problem is that, except for provisions reconciling the provisions of this bill with the provisions of the Children's Online Privacy Protection Act and certain provisions of the Federal Communications Act, there are no provisions reconciling the proposed legislation with other important Federal privacy legislation. For example, it is unclear how S. 2201's requirement of notice and "opt-in" choice for disclosure of financial information collected online would be reconciled with GLB's notice and "opt-out" requirements for the same information. Nor is it clear whether a credit reporting agency's use of a website to facilitate communications with its customers would subject it to a separate set of notice, access, and security requirements, beyond those already in the Fair Credit Reporting Act.

I want to emphasize that I note these examples, not to criticize the drafting of the proposed legislation, but to illustrate the inherent complexity of what it is trying to accomplish.

---

[1] There may be areas in which new legislation is appropriate to address a specific privacy issue. This letter addresses my concerns about broad, general legislation governing online privacy issues.

[2] I am unaware of any evidence that the passage of GLB increased consumer confidence in the privacy of their financial information. In contrast to GLB's notice requirements, certain GLB provisions targeting specific practices have directly aided consumer privacy. For example, the law prohibits financial institutions from selling lists of account numbers for marketing purposes, and makes it illegal for third parties to use false statements ("pretexting") to obtain customer information from financial institutions in most instances.

[3] The Committee's Final Report is available at *www.ftc.gov/acoas/papers/finalreport.htm.*

2. The legislation would have a disparate impact on the online industry.

Second, I am concerned about limiting general privacy legislation to online practices. Whatever the potential of the Internet, most observers recognize that information collection today is also widespread offline. Legislation subjecting one set of competitors to different rules, simply based on the medium used to collect the information, appears discriminatory. Indeed the sources of information that lead to our number one privacy complaint—ID Theft—are frequently offline. Of course, applying the legislation offline would increase the complexity of implementation, again underscoring the difficulties inherent in general privacy legislation.

3. We have insufficient information about costs and benefits.

Third, although we know consumers value their privacy, we know little about the cost of online privacy legislation to consumers or the online industry. Again, the experience under GLB indicates that the costs of notice alone can be substantial. Under S. 2201, these costs may be increased by the greater number of businesses that must comply, by uncertainty over which set of consent procedures apply, and by the difficulty of implementing access and security provisions.

4. Rapid evolution of online industry and privacy programs is continuing.

Fourth, the online industry is continuing to evolve rapidly. Recent surveys show continued progress in providing privacy protection to consumers. [4] Almost all (93 percent) of the most popular websites provide consumers with notice and choice regarding sharing of information with third parties. Some of the practices of most concern to consumers, such as the use of third party cookies, have declined sharply. Moreover fewer businesses are collecting information beyond email addresses. These changes demonstrate and reflect the more important form of choice: the decision consumers make in the marketplace regarding which businesses they will patronize. Those choices will drive businesses to adopt the privacy practices that consumers desire.

Perhaps most important for the future of online privacy protection, 23 percent of the most popular sites have already implemented the Platform for Privacy Preferences (P3P). This technology promises to alter the landscape for privacy disclosures substantially. Microsoft has incorporated one implementation of P3P in its web browser; AT&T is testing another, broader implementation of this technology. By the time the Act's disclosure regulations might reasonably take effect, [5] the technological possibilities for widespread disclosure may differ substantially. Although S. 2201 anticipates this development by requiring the National Institute of Standards to promote the development of P3P technology, legislation enacted now cannot take advantage of such nascent technology. Moreover, it may inadvertently reduce the incentives for businesses and consumers to adopt this technology if disclosures are required using other approaches.

5. Diversion of resources from ongoing law enforcement and compliance activities.

Finally, there is a great deal the FTC and others can do under existing laws to protect consumer privacy. Indeed, since 1996, five new laws have had a substantial impact on privacy-related issues. [6] We should gain experience in implementing and enforcing these new laws before passing general legislation. Implementation of yet another new law will require both industry and government to focus their efforts on a myriad of new implementation and compliance issues, thus displacing resources that might otherwise improve existing privacy protection programs and enforce existing laws. Simply shifting more resources to privacy related matters will not, at least in the short term, correct this problem. The newly-assigned staff would need to develop the background necessary to deal with these often complex issues. The same is likely true for business compliance with a new law. Without more experience, we should opt for the certain benefits of implementing our aggressive agenda to protect consumer privacy, rather than the very significant effort of implementing new general legislation.

---

[4] The Progress and Freedom Foundation recently released the results of its 2001 Privacy Survey, available at *www.pff.org/pr/pr032702privacyonline.htm.*

[5] Again, GLB is instructive. It was almost two years between the enactment of the statute and the effective date of the privacy rules promulgated thereunder.

[6] Fair Credit Reporting Act, 15 U.S.C. §1681 (amended 9/30/96); Health Insurance Portability and Accountability Act, 42 U.S.C. §1320 (enacted 8/21/98); Children's Online Privacy Protection Act, 15 U.S.C. §6501 (enacted 10/21/98); ID Theft Assumption & Deterrence Act, 18 U.S.C. §1028 (enacted 10/30/98); GLB, 15 U.S.C. §6801 (enacted 11/12/99). Moreover, since 1996, the FTC has been applying its own statute to protect privacy.

Conclusion

We share the desire to provide American consumers better privacy protection and to ensure that American businesses face consistent state and Federal standards when handling consumer information. Nonetheless, we believe that enactment of this general online privacy legislation is premature at this time. We can better protect privacy by continuing aggressive enforcement of our current laws.

Sincerely,

TIMOTHY J. MURIS
Chairman

FEDERAL TRADE COMMISSION
Washington, DC, April 24, 2002

Hon. JOHN MCCAIN,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.

RE: S. 2201 (THE ONLINE PERSONAL PRIVACY ACT)

Dear Senator McCain:

I am pleased to provide my views on S. 2201, the Online Personal Privacy Act, which was introduced by Chairman Hollings on April 18, 2002. Although I share the view of the sponsors of this legislation that privacy is important to American consumers, there has been no market failure that would justify the passage of legislation regulating privacy practices concerning most types of information. Even if such a market failure exists, I am not persuaded that the benefits of such legislation, including the proposed Online Personal Privacy Act, exceed its costs.

Indeed, the best means of protecting consumer privacy without unduly burdening the New Economy is through a combination of industry self-regulation and aggressive enforcement of existing laws that are relevant to privacy by the FTC and other appropriate regulatory agencies. This approach is flexible enough to respond rapidly to technological change and to the tremendous insight we are gaining from the ongoing dialogue among government, industry, and consumers on privacy issues.

You have asked for my assessment of whether legislation is needed. I believe legislation should be reserved for problems that the market cannot fix on its own. To my knowledge, there is no evidence of a market failure with respect to online privacy practices, nor are there signs of impending market failure that would warrant burdensome legislation. As a result of a continuing and energetic dialogue among industry, government and consumer representatives, industry is stepping up to the plate and leading the way toward enhancing consumer privacy online. Flexible and efficient privacy tools are increasingly addressing consumer concerns. Indeed, the evidence indicates that the market is responding to consumers' concerns and demands about privacy.

A recent Progress and Freedom Foundation study [1] tells us that there has been a significant decline in the amount of personal information that websites are collecting from visitors. [2] At the same time, there has been an increase in the voluntary adoption of privacy practices. The study indicates that privacy policies have become more common and more consumer-friendly over the past year. In addition, the percentage of the most popular sites offering consumers a choice whether their information can be shared with third parties increased from 77% in 2000 to 93% in 2001. The privacy-enabling technology, Platform for Privacy Preferences (P3P), is being deployed rapidly, and industry has generally become more responsive to the privacy concerns of consumers.

These trends clearly demonstrate that the online marketplace is dynamic, and that firms are working hard to find the "right" pattern for information management practices. In addition, the survey results show that the most frequently visited websites (and much of the Internet as a whole) have clearly recognized that information management policies and privacy practices are necessary parts of everyday business on the Internet. Consumers expect privacy protection and firms realize

---

[1] Adkinson, William F. Jr., Jeffrey A. Eisenach, Thomas M. Lenard, Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites. Washington, D.C.: Progress & Freedom Foundation (2002). Available at: *http://www.pff.org/publications/privacyonlinefinalael.pdf.*

[2] Among the most popular 100 sites, the proportion collecting personal information fell from 96% in 2000 to 84% in 2001. Similar to this finding, the proportion of those firms employing "cookies" fell from 78% to 48% in the past year.

that it is to their competitive advantage to respond to customer expectations. To the extent that consumers have demanded privacy, these results show that the market has provided it.

Contrary to arguments by proponents of legislation that consumers' privacy concerns are retarding the growth of electronic commerce, electronic commerce is growing rapidly without new privacy legislation. Online transactions have roughly doubled each year between 1997 and 1999, and annual consumer purchases have risen from roughly $5 billion in 1998 to $32 billion in 2001. Recent data on online holiday shopping are even more dramatic, rising from roughly $1 billion in 1997 to nearly $14 billion in 2001—a 1300% increase. E-commerce thus is growing rapidly in the absence of new privacy regulation. [3]

For many years now, it has been my understanding that Congress seeks to weigh the costs and benefits of new legislation, with the goal of avoiding doing more harm than good. To my knowledge, there is no evidence concerning the costs associated with the proposed legislation, nor an assessment of whether those costs are outweighed by the ill-defined economic benefits that might follow. I do not believe legislation should be adopted without careful consideration of the problems it may create.

Perhaps the most glaring cost associated with the bill, and with any online-specific privacy legislation, is that it discriminates in favor of offline commerce. It is important to remember that electronic commerce currently constitutes a very small portion of all commercial activity. It is difficult to understand drawing a distinction between offline and online privacy. I would suggest that it is likely that consumers share similar concerns in both situations. I believe it is essential to consider the costs and benefits of regulating both online and offline privacy before any legislation is enacted.

To evaluate other costs associated with the notice and choice requirements of the Online Personal Privacy Act, the Commission's experience with the Gramm-Leach-Bliley Act (GLB Act) is instructive. The GLB Act requires that financial institutions issue privacy notices to their customers and, in certain circumstances, provide them with the opportunity to opt out of disclosures of nonpublic personal information to nonaffiliated third parties. To comply with the GLB Act last year, firms incurred great expense in disseminating privacy notices, yet very few consumers opted out. Among the difficulties encountered in complying with the GLB Act was the challenge of communicating complex information to consumers. Industry would face these same challenges in communicating notice and choice in the online context, and a requirement to provide "robust" notice to consumers does little to solve these problems. It also would be difficult for static regulation to keep pace with technology. For example, regulation mandating notice provided on a website may be inapplicable to Web-enabled handheld devices, such as cell phones.

A requirement to provide "reasonable access and security" is difficult to define. In its May 2000 report, the Commission's Advisory Committee on Online Access and Security was unable to reach consensus as to the amount and type of access that should be provided to consumers. [4] Given the complexity of this issue, I do not believe that it is a suitable topic for broad-based legislation or regulation. More important, the Commission already has the ability to address security breaches through the enforcement of existing statutes. [5]

In addition, I am not aware of reliable information about the likely costs associated with providing access and, in particular, the costs of maintaining a clickstream database that could be easily accessible to consumers and easily altered. [6] I there-

---

[3] It is interesting to compare the growth of electronic commerce to the growth in the use of debit cards. Between 1988 and 1996, debit transactions slowly rose from virtually nothing to less than $50 billion annually. As consumers' experience with these cards increased, however, debit card spending jumped to $300 billion in 2000. This massive growth in debit card transactions was not caused by federal regulatory action, but resulted from consumers' positive experiences with the cards.

[4] In 1999, the Commission established an Advisory Committee on Online Access and Security to provide advice and recommendations to the Commission regarding implementation of reasonable access and adequate security by domestic commercial websites. The Committee's final report to the Commission on May 15, 2000, described options for implementing reasonable access to, and adequate security for, personal information collected online and the advantages and disadvantages of each option.

[5] *See* In the Matter of Eli Lilly and Co., FTC File No. 012 3214 (consent agreement accepted, Jan. 17, 2002) (alleging that Eli Lilly unintentionally disclosed personal information collected from consumers by not taking appropriate steps to protect the confidentiality and security of that information).

[6] Under the proposed legislation, clickstream data, as collected by third-party cookies, are considered to be personally identifiable information to which consumers should have access.

fore question whether the $3.00 fee allowed by S. 2201 for consumers to obtain access to their information would be sufficient to cover the expense. Although some firms—obviously the larger ones—might be able to absorb the costs associated with this access mandate, other firms might be unable to provide the service for a minimal fee and would be unable to continue business with their current model. This possibility seems terribly unfair to small business and harmful to competition in electronic commerce.

Finally, in an attempt to empower consumers, this legislation gives them a private right of action. While this measure is aimed at increasing compliance with the law, I fear that a private right of action may result in unintended consequences. More specifically, increased private litigation over information management policies may chill further innovation on the part of businesses that may fear that any change in their information management practices will be met with lawsuits.

In summary, the electronic marketplace is still evolving. Industry and government have been working diligently to address consumers' privacy concerns. Businesses have made admirable progress over the past several years and have no intention of standing down. Industry leaders are directly involved in seeking solutions to meet consumer demands and concerns. From a business standpoint, it just makes good sense. Now is not the time for the federal government to legislate and effectively halt progress on these self-regulatory efforts. New, complicated, and ambiguous laws will force innovation and investment to take a back seat to compliance and bureaucratic process. At the end of the day, we will have made far less progress in finding solutions to privacy concerns than we would have if we had simply relied on government and private sector cooperation and market forces.

Thank you for the opportunity to offer my views on these issues. I look forward to working with you in the future.

Sincerely,

ORSON SWINDLE,
Commissioner

FEDERAL TRADE COMMISSION
Washington, DC, April 24, 2002

Hon. JOHN MCCAIN,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.

RE: S. 2201 (THE ONLINE PERSONAL PRIVACY ACT)

Dear Senator McCain:

In anticipation of the Senate Commerce Committee's April 25, 2002 hearing on S. 2201, the Online Personal Privacy Act ("OPPA"), you have asked each Commissioner of the Federal Trade Commission to comment on whether legislation is needed and, if so, what such legislation should contain. As you know, the FTC has long been involved with the issue of consumer privacy and I have also personally devoted a great deal of time and thought to this matter. Accordingly, I appreciate the opportunity to offer my views about privacy legislation and comment on the principal features of the OPPA.

In the past, a particular area of focus for me has been the question of whether federal legislation is necessary. In the Commission's May 2000 Congressional Report, "Privacy Online: Fair Information Practices in the Electronic Marketplace," a majority of the FTC recommended that Congress enact online privacy legislation. In my accompanying statement and written testimony, I expressed my support for thoughtful and balanced online privacy legislation that is coupled with meaningful self-regulation and enforcement of existing laws. [1]

I also stated that such privacy legislation should incorporate the well-established fair information practice principles of notice, choice, access and security and should provide for federal preemption of inconsistent state laws. Further, legislation should be organic and sufficiently flexible to take into account the type and sensitivity of the data at issue.

---

[1] This position represented a change from my prior opinion which did not support legislation but, instead, called for industry self-regulatory measures. *Compare* Statement of Commissioner Mozelle W. Thompson Before Senate Comm. On Commerce, Science and Transp. (May 25, 2000), *with* Statement of Commissioner Mozelle W. Thompson Before Senate Comm. On Commerce, Science and Transp. (July 13, 1999).

My conclusion has not changed and, as discussed below, I believe that today's market conditions make an even more compelling case for legislation. Moreover, I support the OPPA because it contains the above described elements and represents a thoughtful, balanced and well-reasoned approach to the privacy issue.

On-line Privacy Legislation Is Needed

Consumer confidence is one of the most important features of American economic strength and, as demonstrated by recent declines in dot-com industries, emerging markets and young industries are particularly vulnerable to consumer uncertainty. It is not surprising then, that those industries involved in the developing electronic marketplace, or "e-commerce," have begun to direct greater attention and more resources to strategies that address consumer confidence. Members of this industry are asking what is needed to allow e-commerce to reach its potential and fully develop into a stable and robust market? One answer is data privacy.

Studies continue to indicate that consumers' foremost concern with respect to e-commerce is the privacy of their personal data. Indeed, last year Forrester Research estimated that consumers' online privacy concerns cost $15 billion of potential e-commerce revenue. Also, 73% of online consumers who refused to purchase online did so because of privacy concerns. Moreover, one need only compare the stock prices of those companies engaged in online profiling, before and after settling complaints about their business practices, to find a clear example of the value to consumers of certainty and confidence in a new market.

To date, the FTC has provided a strong privacy foundation by way of the agency's law enforcement regime combined with our efforts in promoting industry self-regulation. Although consumers and businesses involved in e-commerce have benefitted from these efforts, they are no longer sufficient because there are still online companies that fail to protect consumer information. Without a legislative backdrop, too much of the risk of e-commerce is shifted to the consumer at a time when consumer confidence is critical. Law enforcement measures are by their nature retroactive, focusing on events that have already occurred. Once a consumer has lost his or her privacy—be it through identity theft, the creation of an unauthorized profile based upon the consumer's online activities or by some other means—it is generally impossible to make that consumer whole again.

This condition is made more serious because the Internet allows instantaneous, inexpensive and unlimited transmission of data while computer databases permit storage and unprecedented manipulation. Moreover, it is difficult for the consumer to even know that his or her privacy has been violated until, in some cases, years after the fact.[2] Consequently, without legislation, e-commerce will remain an uncertain marketplace in which only those consumers on the fringe will participate.

The absence of legislation also forces the Commission into the unusual position of going after the good actors that have strong privacy policies, while the bad remain largely unreachable by agencies like the FTC, thus leaving these businesses free to violate consumer trust. Without the type of legislative backdrop that the Commission called for in 2000, and which OPPA provides, I am afraid there will continue to be many free riders and companies with inadequate information practices.

Necessary Elements For Effective Privacy Legislation

I believe that the OPPA addresses many of the most delicate problems associated with a legislative privacy framework. First, it contains the fair information principles and allows for flexibility and change. The OPPA avoids a "one size fits all" approach to the notice requirements and provides a reasonableness test for access. The OPPA is also more reflective of a "real world" consumer environment because it employs a sliding scale that affords more protection to more sensitive information.

Second, by preempting state law, the OPPA will prevent the possibility of multiple standards that could "Balkanize" e-commerce and prove overly burdensome to business and too confusing for consumers. Finally, in granting the FTC rulemaking authority, the OPPA will permit strong enforcement, with special sensitivity to industry and consumer needs, while also providing a means for state participation.

Thank you again for providing me with this opportunity to discuss privacy legislation and the OPPA. I also hope that you will continue to consider the FTC a resource as your work progresses on this important issue.

Sincerely yours,

---

[2] These features, coupled with technology that allows websites to surreptitiously collect consumer information, distinguish the online consumer environment from the offline world.

MOZELLE W. THOMPSON,
Commissioner

FEDERAL TRADE COMMISSION
Washington, DC, April 24, 2002

Hon. JOHN MCCAIN,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Senator McCain:

Thank you for your letter of April 19, 2002 asking me to comment on Chairman Hollings Senate Bill 2201, "The Online Personal Privacy Act." Your letter asked two questions: First, whether I believe legislation is needed, and if so, what it should contain. Second, you asked for my comments on the principal features of S. 2201.

I. Is legislation needed?

Yes, legislation is needed to protect consumers' privacy. Absent federal standards to be followed by all persons and entities that collect private information, it is unlikely that consumers will be adequately protected from identity theft, commercial harassment, and hucksterism. In addition, dissatisfaction with and mistrust of online business practices by the American people will continue to grow; an uneven patchwork of state laws will proliferate; and consumer confidence in e-commerce will be undermined.

Industry has not been able or willing to effectively self-regulate. While some responsible companies have stepped up to the plate, the financial incentives work against a universal commitment by e-business to provide *effective* privacy protection for consumers. Business interests will undoubtedly point to a recent Progress and Freedom Foundation survey as evidence that federal legislation is not necessary because websites are collecting less personally identifiable information and privacy notices are prevalent, more prominent, and more complete. These arguments completely miss the mark. First, the survey reveals that nearly all sites surveyed continue to collect personally identifiable information.[1] Second, the mere posting of a privacy policy does not ensure *effective* consumer protection and often is only pretty packaging of empty content.

Just any legislation is not enough. In my view, strong privacy legislation should:

- preempt inconsistent or weaker state law;
- incorporate effective notice and choice, adequate access, reasonable security, and strong enforcement remedies;
- be free from exceptions created for special interests or industries;
- require affirmative consumer consent before sensitive personally identifiable information is collected through any means either online or offline; and
- avoid tactics that unduly delay the effective date of the Act.

II. Senate Bill 2201

Senate Bill 2201 provides long-awaited, strong protection measures for consumers in the online world. My only concern with this proposed legislation is its limited reach. In my view, federal legislation is necessary to protect the privacy of personally identifiable consumer information in the *offline* as well as online commercial realms. These marketplaces are often intertwined and indistinguishable. In fact, I believe that the wired world facilitates the effective, constant aggregation of endless varieties of real-time "surfer" information and combines it with commercial information gathered through traditional "offline" means. I would strongly support the expansion of this Bill's consumer protections to the "offline" collection of personally identifiable consumer information.

That said, Senate Bill 2201 is a balanced, comprehensive approach to protecting consumer privacy *online.* By incorporating the concepts of notice, choice, access, security, and enforcement, it creates a level playing field for both consumers and industry. However, I offer the following comments:

---

[1] The survey indicated that 90 percent of the random sample, and 96 percent of the most popular sites, collect personally identifiable information compared with 97 percent and 99 percent in 2000. This is hardly a statistically significant decline. In fact, an April 11, 2002, *New York Times* article (attached) chronicled how some of the Internet's most frequently visited sites are expanding their collection and commercial use of personally identifiable information.

Preemption

I believe that federal legislation should preempt inconsistent and weaker state privacy laws which do not effectively protect consumers and tend to frustrate the development of e-commerce. On the other hand, I generally support the power of states to enact legislation that offers their citizens stronger consumer protections than federal law where the federal law merely establishes a "floor" of minimum protection standards. However, if passage of a federal law "with teeth," is feasible, I believe that both consumers and industry would value the uniformity and predictability that federal preemption offers.

Title I—Online Privacy Protection

Section 101

I applaud Title I's coverage of personally identifiable information that is collected, *used* or *disclosed.* Previous bills focused only on the "collection" of information, yet many privacy breaches occur when information is used or disclosed without the consumer's knowledge or consent after collection.

Notice and Consent

I strongly support the inclusion of Section 102(b) which requires a consumer's affirmative consent ("opt-in") before, or at the time that, certain sensitive information is collected. An opt-in consent requirement guarantees consumer notice and meaningful choice, and compels the collector to clarify its practices in order to entice the consumer to agree to them. It effectively equalizes the bargaining position of consumers and e-merchants in the market for personal information.

While I prefer an opt-in standard for the collection of *all* personally identifiable information, the Bill's requirement of robust notice and opt-out consent for nonsensitive personally identifiable information improves on the level of notice and choice currently provided by many websites. Also, I support the permanence of consent provision found in Section 102(e), which essentially provides that a consumer's privacy preferences stay with the user despite corporate changes.

Section 103's requirement that changes in privacy policies or the existence of privacy breaches be communicated to consumers is particularly commendable. Many websites place the privacy protection burden on consumers to keep track of changes in a website's privacy policy. Section 103 appropriately places that responsibility on the internet service provider, online service provider, or operator of a commercial website. Likewise, the Bill's provision requiring user notification of material changes in the privacy policy allows consumers to utilize updated, relevant information when deciding how or whether to protect their own personal information. Section 103 illustrates the balanced approach of this Bill to the extent it acknowledges that there may be situations where delayed consumer notifications is appropriate.

The exceptions contained in Section 104 seem reasonable and again reflect the Bill's inherent respect for the need to balance the vital privacy interests of consumers with the economic and financial interests of e-business.

Access

The access provision of Section 105 appropriately enables consumers to suggest corrections or deletions of personally identifiable information that the provider or operator has collected or combined with personally identifiable information gathered from other sources. The reasonableness test incorporated in this section strikes an appropriate balance among the competing interests of consumer privacy, the relative sensitivity of different types of personal information, and the burdens and costs imposed on the website operator.

Security

The security provision in Section 106 is consistent with the approach taken by the Commission in its Gramm-Leach-Bliley Act Security Rulemaking. Rather than dictate a one-size-fits-all solution, it is up to the website to establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of the data it maintains.

Title II—Enforcement

I am impressed with the range of remedies included under this Title, including the authority to impose civil penalties and establish redress funds for consumers for violations of Title I. In addition, this Title allows private rights of action as well as state actions.

Title III—Application to Congress and Federal Agencies

To my knowledge, the federal agencies do not trade in private consumer information for commercial purposes. Therefore, I see no justification for Section 302. How-

ever, I do believe that federal agencies should provide notice to consumers about their information collection practices consistent with applicable federal law.

Title IV—Miscellaneous

Section 402 provides that the effective date of the Act will be the day after the date the Commission publishes a final rule under Section 403. While I am pleased that there is no "grace period" for compliance with this Title, I am disappointed that data collectors will be free from liability for data they collected *without* consumer consent *before* the Act's effective date. I also hope that Congress will resist obvious delaying tactics, such as proposals for additional studies.

Technical concerns

Section 403 may need technical modifications to achieve the Bill's goals. Our staff would be pleased to assist you in these efforts. Specifically, Section 403 should reflect that the rulemaking contemplated by the Act is to be conducted pursuant the Administrative Procedures Act rather than through a Magnuson Moss Rulemaking.

I appreciate the opportunity to express my views, and I hope they are helpful.

Sincerely,

SHEILA F. ANTHONY,
Commissioner

FEDERAL TRADE COMMISSION
Washington, DC, April 24, 2002

Hon. JOHN MCCAIN,
Ranking Member,
Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Senator McCain:

You have asked that members of the Federal Trade Commission provide their individual views on a privacy bill, "The Online Personal Privacy Act," S. 2201, and I am pleased to respond.

It is important to express a key reservation up front. This statement of my individual views is constrained by my understanding of the context of your request. Like any other citizen, I have personal views on fundamental issues in the privacy debate (e.g., the question of whether it is appropriate to speak of a "right to privacy" in the context of private consensual transactions as opposed to intrusions by government; the balance between any privacy rights of one party and the First Amendment rights of another; and the question of whether it is realistic to expect that most barriers to disclosure will prove effective in the long term). However, there is no reason why you or any other lawmaker should be particularly interested in my opinions about these value-laden issues, so I understand that you are asking for my views in the context of the responsibilities and capabilities of the Federal Trade Commission. In other words, this response is constrained by an appreciation of the limitations of our institutional expertise. [1]

To be blunt, I do not believe it is my place to advise Congress on the bottom line issue of whether it is or is not a good idea to legislate on privacy issues. (To the extent I presumed to do so in the past, I have changed my mind.) The Federal Trade Commission, in my view, functions best as a facilitator, which attempts through law enforcement and education [2] to ensure that consumers are not misinformed about the goods and services that they buy and that sellers are not disabled by illegal private constraints. But, in the absence of Congressional direction to the contrary, we are neutral about the terms of sale that are freely determined. We have strong institutional confidence in the ability of adequately informed consumers to make their own choices about what they want (including, presumably, varying levels of privacy protection) without interference from government. We are good at specifying what is adequate disclosure of the terms of sale but we are not good at devising rules for what the terms of sale should be.

With this awareness of our limitations, I join with those colleagues who express serious reservations about the "Online Personal Privacy Act," S. 2201. I generally concur in their conclusions, but write separately to emphasize my particular perspective. I simply do not believe that S. 2201 can be enforced in a coherent way. The following is a summary list of the reasons:

---

[1] My previous statements on privacy issues are enclosed with this letter.

[2] The Commission also provides a forum for the exchange of views among outside individuals and groups.

1. I do not believe it is workable or reasonable to treat privacy differently in the online world than in the offline world *to the extent that the information collected is the same,* regardless of the site of collection or the means of dissemination. It is obvious that different modes of disclosure might be required, but it is illogical to regulate one medium and not the other.

2. Congress may, in its judgment, determine that it is appropriate to mandate some form of "notice" to consumers about what will happen to their personal information. For one thing, mandated notice would eliminate the present awkward situation whereby a company that volunteers information about its privacy policy [3] risks prosecution if the information is inaccurate, but one that volunteers nothing risks nothing. [4] Recent experience with mandated notice, however, suggests that it is not enough for Congress simply to require that it be done. [5] Businesses have to be given more precise guidance about the forms of notice that will be useful to consumers. This is something that the Federal Trade Commission, as an institution, knows something about. It might be appropriate to direct the Commission or some other appropriate body to survey the *quality* of notices that are either voluntarily provided or mandated today, and then recommend a template for notice that would be meaningful. This project would inform the policy debate and ultimately, perhaps, provide the framework for legislation.

3. The issue of "choice" or "consent" is much more complex than the bill seems to recognize. At first glance, it seems obvious that the whole purpose of notice is to enable consumers to make informed choices. It is necessary, however, to think about *the consequences of choice.* If there is no cost or reduced benefit associated with the choice to opt-out (or failure to opt-in), then the added expense of accommodating these choices will be borne by consumers less tender of their privacy. (No one suggests that people who do not want to use their supermarket charge cards because of the information disclosed should be entitled to the discount anyway.) On the other hand, if privacy-conscious consumers are disadvantaged too much, their only practical "choice" is to seek another provider, and mandated "opt-outs" or "opt-ins" become essentially meaningless. There would have to be some regulatory regime to determine what is a reasonable in-between position in these circumstances, and I have no idea how this could be done across-the-board.

4. Under the bill, further refinements of "access" and "security" would presumably need to be spelled out in rulemaking proceedings. [6] As I have said before, "[i]t is not appropriate to defer all the tough issues for future rule-making." [7] I personally believe, for example, that there is a vast disparity between the costs and benefits of an access regime in most situations, and I further believe that the costs of merely developing and enforcing across-the-board rules would also vastly exceed the benefits. Congress may want to consider whether any tailored expansion of present rights is necessary, [8] but a blanket mandate of "access" rights is unlikely to result in significant benefits overall.

These are major objections, but the following issues are also significant:

5. S. 2201 distinguishes "sensitive" from "non-sensitive" personal information. [9] These categories seem arbitrary. For example, as Chairman Muris points out in his letter to you of this date, some might feel that information about the books they read is a lot more sensitive than their political affiliation. Moreover,

---

[3] And, apparently, an overwhelming majority do, according to the most recent evidence. William F. Adkinson, Jr., Jeffrey A. Eisenach and Thomas Lenard, Progress & Freedom Foundation, "Privacy Online: A Report on the Information Practices and Policies of Commercial Websites" *www.pff.org/pr/pr032702privacyonline.htm.*

[4] The vendor may, of course, incur marketplace risk.

[5] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6810; and Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices (December 4, 2001) *http://www.ftc.gov/bcp/workshops/glb/index.html.*

[6] S. 2201, Section 403.

[7] Federal Trade Commission, "Online Profiling: A Report to Congress" (Part 2) (Statement of Commissioner Thomas B. Leary, Concurring in Part and Dissenting in Part)(July 2000) *http://www.ftc.gov/os/2000/07/onlineprofiling.htm#LEARY.*

[8] The Fair Credit Reporting Act , 15 U.S.C. §§ 1681 et seq., and the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 et seq., are among the federal laws that grant access rights.

[9] S. 2201, Sections 102 and 401.

information that is merely "inferred" from data [10] may be just as sensitive as information "about" [11] certain aspects of an individual. [12]

6. The distinction between "clear and conspicuous" notice and "robust" notice [13] seems unworkable as a legal mandate. Articulation of the latter undercuts the significance of the former. If some form of notice is ever mandated by Congress, it should be both.

7. The bill is silent about the extent to which privacy protections travel with consumers' personal information. In general, Gramm-Leach-Bliley's privacy provisions require downstream recipients of covered data only to use the information in a fashion that is consistent with the consumers' stated privacy preferences or only for uses that are exempted from the notice and choice requirements (such as credit reporting). In this sense, the protections flow with the information. I seriously question whether this concept can be applied across the economy, but without it, the privacy protections of the bill may be nullified.

8. As Chairman Muris notes, some of the provisions of S. 2201 attempt to reconcile the legislation's privacy protections with other federal statutes that allow limited but beneficial information sharing. However, as currently drafted, S. 2201 might limit a variety of legitimate and beneficial information sharing which covered entities engage in and which Congress would like to continue. It is not clear, for example, whether information about transactions completed online could be communicated to credit bureaus. Without appropriate exclusions, any proposed privacy rules could have a serious anti-consumer impact.

9. This bill would add to the emerging patchwork of federal privacy regulations that apply to personal information [14] and may ultimately result in ambiguous, conflicting, or impractical requirements for businesses, and greater confusion for consumers as well. For example, S. 2201 provides that "sensitive" and "non-sensitive" information would be subjected to different levels of protection. Dissemination of "sensitive" information would be subject to consumer notice, opt-in choice, access and security. "Non-sensitive" information would be protected by "robust" notice, opt-out choice, access and security. The specifics of these requirements would all be defined in a future rulemaking. At the same time, "non-public" personal information collected by financial institutions (whether online or offline) would be subjected to Gramm-Leach-Bliley's distinct notice, choice and security standards.

Businesses that seek to comply with both of these regulations would be required to differentiate between online and offline information as well as any possible differences between the notice, choice, and security requirements in the two regulatory schemes. Additionally, our experience to date with Gramm-Leach-Bliley suggests that consumers may need *less* rather than *more* complex privacy disclosures in order to understand and execute their rights. It is unrealistic, at this point, to assume that consumers will comprehend the various categories of information as well as the protections that are attached to each category of information.

10. The bill provides that "penalties" would be imposed for a violation of the statute, and that "redress" would be distributed to consumers in an amount not to exceed $200 (for breaches involving non-sensitive personal information). This confuses two separate concepts. Penalties are calculated without regard to con-

---

[10] S. 2201, Section 401.

[11] S. 2201, Section 401.

[12] See, In the Matter of Eli Lilly and Co., FTC File No. 012–3214 (January 18, 2002) *http://www.ftc.gov/opa/2002/01/elililly.htm.* This case involved the improper disclosure of the identity of people who had regularly obtained information about a certain psychotropic medication, but did not disclose whether they actually took the medication.

[13] S. 2201, Sections 102 and 401.

[14] Among the many federal privacy laws are: Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6810 (covers financial institutions, non-public personally identifiable information and requires notice of information practices and an opt-out for sharing information with third parties); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 et seq. (covers Web site operators, prohibits collection, use and disclosure of children's online information without verifiable parental consent and provide for parental access rights and imposes security requirements); Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. (covers credit bureaus and providers and users of credit data and grants consumers access rights and opt-out rights for certain uses of credit data); and Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 262(a), 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.A.); 42 U.S.C.A. §§ 1320d to 1320d–8 (West Supp. 1998)(covers a variety of health-related entities and health information and contains requirements that include notice, varying degrees of choice, access, and security).

sumer injury or ill-gotten gains, and are paid to the Treasury. Redress is intended to make consumers whole.

11. Wholly apart from the burden issues identified above, the bill does not seem to recognize the potential conflict between access and security. Broad access rights will lead to the centralization of data which could result in very significant security breaches. This is a highly technical subject, on which there is no consensus among experts. [15]

I appreciate the opportunity to provide these comments and would be pleased to respond to any further questions.

Sincerely,

THOMAS B. LEARY,
Commissioner

The CHAIRMAN. Senator Cleland.

STATEMENT OF HON. MAX CLELAND,
U.S. SENATOR FROM GEORGIA

Senator CLELAND. Thank you very much, Mr. Chairman.

The difference between the world we see today and the world we saw last year is quite stark. Given September 11, the support for our men and women fighting in uniform, fighting terrorism abroad, for law enforcement efforts to uncover terrorist activity at home have justifiably received support, and I fully support these efforts as well, but on the domestic front, protecting people's privacy at home still remains for me an important issue as well.

I am constantly reminded of this fact from stories of people who provide incorrect information to online businesses because of the fear that this information may be improperly used and from consumers choosing to bypass the many services the Internet provides for commercial purposes because they are concerned their online buying habits may be shared with others.

The Senate has acted in a manner which I believe is balanced in its approached to online privacy. S. 2201, the bipartisan privacy legislation of which I am a proud cosponsor, incorporates many of the concerns of the high tech industry and balances those with a need of protections that have been advocated by civil liberties groups.

Under the bill, sensitive information such as financial and health records, ethnic information, religious affiliation and social security numbers must be protected unless a person provides affirmative consent that this information can be shared. Other nonsensitive information can be shared between companies unless the consumer opts out of this sharing. That is straightforward protection in its most basic form, and, like the Fair Credit Reporting Act, which has worked well for consumers, information will be accessible and correctable. This approach is reasonable, as evidenced by the bipartisan support it has received.

I believe that one of Yahoo's former vice presidents for direct marketing correctly frames the issue when he describes Yahoo's recent change in its privacy policy that would require opting out of receiving solicitations. Quote, they would be better off sending offers to a million people who said they want to receive a coupon

[15] Final Report of Federal Trade Commission Advisory Committee on Online Access and Security, published as Appendix D of Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (May 2000) *http://www.ftc.gov/acoas/papers/finalreport.htm.*

each day, than to send them to 10 million people and worry about whether you have offended them by finally going too far. This is basic marketing knowledge, and I see no reason why it should not apply to the Internet as well.

We have a good privacy protection bill for consumers, and I appreciate the opportunity to work with the Chairman on perfecting this legislation. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. We welcome the distinguished panel. Each of the statements of the distinguished witnesses are included in their entireties in the record. The Senators have had a chance to review those statements, and we would ask, in order that we leave some good time for questioning, that each of the witnesses summarize within, let us say, the 7-minute rule. Let me start over on your right and go right across and start with Mr. Torres and end with Mr. Dugan.

Mr. Torres.

STATEMENT OF FRANK TORRES, LEGISLATIVE COUNSEL, CONSUMERS UNION

Mr. TORRES. Good morning, Mr. Chairman, Members of the Committee. Consumers Union appreciates the opportunity to discuss our support for S. 2201. S. 2201 is a sound privacy law that will increase consumer trust and confidence in the online marketplace. We commend you and other members who have sponsored this landmark bill. You and your staffs have worked hard to balance the consumer's interest with those of the tech world, bending over backward in some cases to address their concerns. Here are some of the reasons we believe this bill is good.

First, S. 2201 will provide both consumers and businesses with clear expectations of how online information will be treated, when it can be shared, and let consumers control the use of their personal data. Up till now, privacy has been addressed sector by sector. We often hear complaints from businesses that one sector is being treated differently from another. S. 2201 responds to those concerns. Consumers Union believes that basing the protection trigger on the type of information collected, rather than any specific industry, is the right way to address online privacy.

Second, S. 2201 advances the privacy debate by recognizing the distinction between sensitive and nonsensitive data. More sensitive personal data like financial and medical information warrant the strongest possible protections. A business should first obtain a consumer's consent before protecting or sharing that information outside the scope of the reason for which that data was given.

Where data is less sensitive, a less rigorous approach may be appropriate. However, this only works if the notice is good. The robust notice contemplated in S. 2201 will provide an up-front mechanism for consumers to get privacy notices and exercise their opt-out.

Third, S. 2201 offers a substantial improvement over the Gramm-Leach-Bliley Act by providing that sensitive financial information cannot be shared without the express consent of consumers, again for reasons outside the scope for which it was given.

On the issue of preemption, Consumers Union believes that the strength of S. 2201 must be weighed against State privacy efforts.

S. 2201 could set a strong national standard. However, should the bill be scaled back, we would revisit our position on the preemption issue and the bill as a whole.

Businesses that choose to collect and share sensitive personal information should be held accountable for their handling of that data. This gets to the question of the private right of action. If wrongful disclosure of sensitive data after a consumer has said no leads to identity theft, for example, shouldn't the consumer be compensated for his or her loss?

S. 2201 exercises an abundance of caution on this issue, given the concerns of the industry. It applies only to sensitive data. The consumer must prove actual damages. The amount of damages is limited even for multiple breaches, and actions cannot be brought if the disclosure was caused by systems failure or an event beyond the control of the business.

In fact, there are a number of privacy laws that are both opt-in and also allow consumers to go after the wrong-doers. We have not heard, as I am sure we would have, of any explosions of lawsuits in these areas. We know from privacy surveys that consumers are concerned about privacy. They are more concerned about online than offline privacy. They want Congress to act, and they favor an opt-in approach overall. This bill splits between an opt-in and an opt-out approach. Consumers are concerned about privacy because banks have shared sensitive information with felons, or have used sensitive information fraudulently.

We are here because of Double Click, Toy Smart, and Yahoo and their practices. Maybe some think it is OK for banks to share customer data with felons, or that companies should be allowed to lie to consumers. We, however, believe that such behavior is unacceptable. The reaction of some to S. 2201 and other privacy bills reminds me of the story of Goldilocks. This bill is too hot, or this one is too cold.

Unlike Goldilocks, however, some will never find the privacy law that is just right. They are going to oppose any privacy legislation that Congress offers. S. 2201 gives consumers control over their own information, and it places the burden where it should be, on businesses who want information to convince consumers to share it. Isn't that how the marketplace should be working?

Thank you, and I would be happy to answer any questions.

[The prepared statement of Mr. Torres follows:]

PREPARED STATEMENT OF FRANK TORRES, LEGISLATIVE COUNSEL, CONSUMERS UNION

Consumers Union [1] appreciates the opportunity to present this testimony on the *Online Personal Privacy Act, S. 2201*. This hearing provides a forum to discuss why American consumers need meaningful and comprehensive online privacy protec-

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports*, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

tions, how S. 2201 accomplishes those goals, and Consumers Union's support for the bill.

Introduction

Consumers Union has long been an advocate for strong privacy protections. Along with other consumer and privacy advocates we pushed for amendments to the Gramm-Leach-Bliley Act to try to provide consumers control over how their personal financial information is collected and whether it could be shared. We fought for strong medical privacy regulations and continue to push for privacy related to health like genetic information. Consumers Union is also part of a broad privacy coalition that has supported online privacy protections.

Stronger laws are needed to give consumers control over their personal information. Legislative efforts such as S. 2201 will help ensure that consumers are told about how and why information is collected and used, provided access to that data, and given the ability to choose who gets access to their most intimate personal data.

S. 2201 represents a balanced and reasonable approach to online privacy. The bill reflects where there could be some agreement on the substantive privacy protections of notice, access and consent.

Consumers Union believes that basing the protection trigger on the type of information collected, rather than on any specific industry sector is a right way to ensure consumer data is safeguarded. This is a logical way to consider the privacy issue. Consumers should not have to keep track of all the businesses entities that may be collecting information about them, especially in light of the growing number of cross-industry mergers and the passage of the Gramm-Leach-Bliley Act. S. 2201 provide clear guidance for businesses as well. If you collect and use consumer data covered by the bill, you know what you have to do.

Background

The right to be left alone appears to have been trumped by the pressure exerted by businesses to protect and expand their ability to gather personally identifiable information from consumers. No part of life is left untouched by data collection activities. Financial and medical records, what you buy, where you shop, your genetic code, are all exposed in a privacy free-for-all. Complete strangers can, for a price, have access to your most intimate secrets. Often, consumers have no choice in whether or not information is collected and no choice in how it is used.

Do consumers care about their privacy? You bet they do.

- According to a survey commissioned by STAR, a subsidiary of Powell Tate, conducted by SWR Worldwide, many consumers report they have informed their primary financial institution of their desire to opt out (31 percent) of information sharing. And 40 percent plan to opt out in the next 12 months. This opt out rate is significantly higher than that reported by financial institutions.
- The survey, conducted after September 11, also found that more than half of the respondents (57 percent) expressed concern that their primary financial institution may be sharing personal or financial information with its affiliates or third parties. The majority (59 percent) also reported that their level of concern is about the same as it was a year ago.
- A recent report by KPMG, entitled A New Covenant With Stakeholders: Managing Privacy as a Competitive Advantage, cites a survey of U.S. voters by the Public Opinion Strategies firm last year indicating that strengthening privacy laws to assure that computerized medical, financial or personal records are kept private is the highest-rated issue of concern to voters nationwide.
- KPMG also noted that increasingly, individuals want to choose who does and does not have access to their medical, financial, purchasing, and other personal information. And, if access is needed, individuals would like to be able to specify for what purposes and to what extent access will be granted. They also want specific assurances that the information they consider private is, in fact, kept private by the organizations with which they do business.
- Forrester Research found that 72 percent of consumers participating in a survey last year considered it a violation of privacy for businesses to collect and then supply personal data to other companies. 94 percent of Internet users want privacy violators to be disciplined. 70 percent said that Congress should pass legislation protecting privacy on the Internet. In December, Forrester found 69 percent of Americans worried about their financial privacy.
- Other surveys have estimated that concerns about privacy and lack of trust cost U.S. companies $12.4 billion in 2000 because consumers were reluctant to share their personal information over the Internet.

- A 2001 study by the Markle Foundation found that by more than a 3 to 1 margin (63–19 percent) the public says it is more concerned about companies collecting personal information online than offline.
- Nearly two-thirds of the public, 64 percent, say that the government should develop rules to protect people when they are on the Internet, even if it requires some regulation of the Internet.
- The study also found that the public is looking not only for protection by others, but they want an ability to control their own online experience, and the uses that others might make of what they do online. By a strong 58–37 percent margin, the public prefers an opt-in regime.
- Finally, the survey concluded that the public perceives that the Internet, although useful, is not yet a medium that enables them to hold others accountable when they go online.

All these surveys lead to the same conclusion: the majority of consumers are concerned about the threats to their privacy while online. An Ernst and Young report *Privacy Promises Are Not Enough*, noted that "at the core of this trust issue is the fact that consumers do not trust businesses to protect their privacy or follow their stated privacy policies."

Increasingly, consumers want to choose who does and does not have access to their medical, financial and other personal information. Consumers want to be able to specify for what purposes and to what extent access to their information will be granted. Consumers want assurances that the information they consider sensitive will be kept private by the businesses they use. Often, consumers have no choice in whether or not information is collected and no choice in how it is used. Today, any information provided by a consumer for one reason, such as getting a loan at a bank, can be used for any other purposes with virtually no restrictions.

Comments on S. 2201

There are a number of elements of privacy protection that have become clearer over the course of our involvement in the privacy debate which are reflected in S. 2201:

- A distinction can be made between sensitive and non-sensitive information. **S. 2201 advances the privacy debate by recognizing the distinction between sensitive and non-sensitive data.** We have commented that more sensitive personal data, like financial and medical information, warrant the strongest possible protections. For this type of data we favor an approach that requires a business to obtain the consumer's consent prior to sharing that data.

  For other data collected, a lessor standard may be appropriate. We support this approach only if clear notice is given to the consumer prior to the collection of the data and that the consumer is given the opportunity up front to choose not to have his or her information shared with others. We encourage providing specific and uniform mechanisms for exercising an opt-out.

  For telephone marketing several states are implementing "do-not-call" lists. Even the Direct Marketing Association maintains such a list. A one-stop universal opt-out would be a useful tool for consumers. We anticipate that the Federal Trade Commission will move forward soon on a final rule for a national do-not-call list. Perhaps a similar mechanism for the online world should be encouraged.
- Consumers need a stronger law to protect their personal financial information. **S. 2201 offers a substantial improvement over the privacy provision of the Gramm-Leach-Bliley Act by providing that sensitive financial information cannot be shared with affiliates or third parties without the express consent of the consumers.** S. 2201 would allow financial institutions to share less sensitive data with their affiliates under the opt-out standard.

  The Gramm-Leach-Bliley Act falls far short of providing meaningful privacy protections in the financial setting. Loopholes in the law and in this draft rule allow personal financial information to be shared among affiliated companies without the consumer's consent. In many instances, personal information can also be shared between financial institutions and unaffiliated third parties, including marketers, without the consumers consent.

  Consumers across the country are receiving privacy notices from their financial institutions. Unfortunately these opt outs, in reality, will do little or nothing to prevent the sharing of personal information with others. Other loopholes allow institutions to avoid having to disclose all of their information sharing practices to consumers. In addition, the GLB does not allow consumers to access to the

information about them that an institution collects. While states were given the ability to enact stronger protections, those efforts have met fierce resistance by the financial services industry.

Reports and surveys conducted by the Privacy Rights Clearinghouse show how poorly written and difficult to understand the financial privacy notices are. Despite those obstacles, a recent survey indicates that consumers are choosing to opt-out.

- Consumers' health information should not be shared without their express consent. **S. 2201 protects personal health information across the board—under the bill health information cannot be shared without the prior consent of the consumer.** There appears to be widespread agreement on this principle.

  Consumers should not be put in the position of privacy intrusions when they go online to seek medical advice or information about prescription drugs, for example. Those seeking medical treatment are most vulnerable and should be allowed to focus on their treatment or the treatment of their loved ones, rather than on trying to maintain their privacy. It is unfair that those citizens must be concerned that information about their medical condition could be provided to others who have no legitimate need to see that information.

- **S. 2201 requires notice and consent prior to the sharing of personal information with others.** Online entities that collect personal information should be responsible for providing notice to consumers if they intend to share personal data with others and allow consumers to opt-out of such data collection and sharing third parties.

- **S. 2201 will allow consumers to opt-out of sharing their less sensitive data.** This requirement should be easy to implement, in most cases consumer choice can be provided at the point where the information is collected. The opt-out for less sensitive information is distinguishable from the stricter regime that would apply to more sensitive financial and medical data. An opt-out may be adequate for such information provided that the notice and choice is given up-front, prior to the collection, and is clear and in plain English. Consumers Union believes that the "robust" notice called for in S. 2201 will provide consumers with the type of notice to get the job done and avoid the pitfalls of the financial privacy notices.

  This is a reasonable step. Consider the position of the former Vice President of Yahoo!, Seth Godin, who has written about "permission marketing. He says that about 38 percent of the people that are given a chance to tell his company their interests to get information about things that match their profile do, in fact, opt-in. He goes on to call opt-out a sham.

- **Businesses should be responsible for safeguarding the sensitive data of Internet users if they choose to collect and use that data.** Businesses that collect and share sensitive personal information should be held accountable if that information is shared after a consumer has said no to such sharing of information. For example, if disclosure of sensitive financial data without the consumer's consent is the cause of that consumer's identity being stolen, shouldn't the businesses that sold the information be held accountable and be responsible for that consumer's loss?

The approach in S. 2201 is reasonable on this issue. It provides a private right of action only related to the misuse of sensitive personal data. Even the, the standard is high—a consumer can only recover upon a showing of actual harm. Actions cannot be brought if a systems failure or an event beyond the control of the business caused the disclosure.

We have not seen evidence of an onerous litigation burden despite a number of prior privacy statutes that allow such action. Most of these laws have been on the books for years:

- Section 616 of the Fair Credit Reporting Act—up to $1,000 for knowing or willful noncompliance plus punitive damages and actual damages for negligent noncompliance;

- 47 U.S.C. Section 551 Cable Communications Policy Act—$1,000 or actual damages plus punitive damages;

- Section 2520 of the Electronic Communication Privacy Act—between $500 and $10,000 and actual damages;

- 18 U.S.C. Section 2710 Video Privacy Protection Act—$2,500 in actual damages plus punitive damages;

• 47 U.S.C. Section 227 Telephone Consumer Protection Act—up to $500 for each violation.

- **The strength of S. 2201 must be balanced against any preemption of state law.** In response to consumer concerns about privacy several states are poised to act on these issues. We consider the work of the states vital. Consumers Union believes that it is critical to seek the input from the states, including state attorneys general and legislators, before deciding to preempt state privacy efforts. As long as the underlying privacy standards remain strong, S. 2201 will set a strong national privacy standard. Should S. 2201 be weakened Consumers Union would reconsider its continued support for the bill and urge that states be allowed to pass tougher privacy laws. Let us be clear, should the other provisions in the bill change, we would reconsider our position on preemption. Preempting state law is predicated on getting the strongest possible consumer protection in the underlying legislation.

The Online Marketplace

The ability to collect, share and use data in all sorts of ways boggles the mind. Consumers, in many cases, aren't even aware that data is being collected, much less how profiles about them are created. The information collection overload is particularly troublesome when it becomes the basis for decisions made about an individual—like how much a product or service will cost.

Cross industry mergers and consolidations have given financial institutions unprecedented access to consumers' personal data. Technology has made it possible and profitable to mine that data. No law prevents businesses from using data to choose between desirable borrowers and less profitable consumers the institutions may want to avoid. Special software helps guide sales staff through scripted pitches that draw on a customer's profile to persuade the account holder to buy extra, and in some cases junk products.

Some web-based businesses already seem to be willing to move beyond the privacy wasteland where GLB left consumers. There no longer appears to be a question, for some, of whether consumers should get notice, access, and control over their information. The challenge is how to effectively put these principles into practice.

A May 2000 *Consumer Reports* survey of web sites, *Consumer Reports Privacy Special Report, Big Browser is Watching You*, shows that consumers' privacy is not being protected online. The report also shows that privacy notices at several popular sites are inadequate and vague. This data, as do other recent web surveys, shows the state of consumer privacy online continues to hit or miss.

Privacy policies are not a substitute for privacy protections, especially when some companies don't even follow what is in their policies. Just because a company has a privacy policy does not mean that they follow Fair Information Practices. And consumers are skeptical about self-regulation.

The marketplace is changing daily. The *Wall Street Journal* reports that Time Warner has the names, addresses and information on the reading and listening habits of 65 million households. *USA Today* says Time Warner has access to information about its 13 million cable subscribers and from its other businesses, like Time and People magazine. With so much information, how will the competitiveness of the marketplace be impacted by this merger? Will companies who seek to operate under a higher privacy standard be at a competitive disadvantage and unable to compete against a larger entity that is able to make unrestricted use of the personal information it obtains?

Do Consumers Benefit from Data Sharing?

Financial institutions promised that in exchange for a virtually unfettered ability to collect and share consumers' personal information, that consumers would get better quality products and services and lower prices. This is why, they claimed, consumers shouldn't have strong privacy protections like the ability to stop the sharing of their information among affiliates, or access to that information to make sure its accurate. Let's look at reality.

Bank fees for many consumers continue to rise. Information about financial health may actually be used to the consumer's determent if it is perceived that the consumer will not be as profitable as other customers. Both Freddie Mac and Fannie Mae say between 30 and 50% of consumers who get subprime loans, actually qualify for more conventional products, despite all the information that is available to lenders today. Credit card issuers continue to issue credit cards to imposters, thus perpetuating identity theft, even when it seems like a simple verification of the victim's last known address should be a warning. Instead of offering affordable loans, banks are partnering with payday lenders. And when do some lenders choose not to share

information? When sharing that information will benefit the consumer—like good credit histories that would likely mean less costly loans.

Chase Manhattan Bank, one of the largest financial institutions in the United States, settled charges brought by the New York attorney general for sharing sensitive financial information with out-side marketers in violation of its own privacy policy. In Minnesota, U.S. Bancorp ended its sales of information about its customers' checking and credit card information to outside marketing firms. Both of these were of questionable benefit for the bank's customers. Other institutions sold data to felons or got caught charging consumers for products that were never ordered.

Maybe the right approach is to let institutions that want a consumer's information to be put in a position to convince that consumer that some benefit will be derived from a willingness to give that information up to the institution. Such an approach may increase trust in financial institutions and let consumers have control and choice over their own personal information. The same technology that enables vast amounts of data to be collected can be used to give consumers access to that data. It is a simple thing to tell consumers what is collected and how it is used.

Conclusion

Consumers face aggressive intrusions on their private lives. Often a consumer is forced to provide personal information to obtain products or services. Many times information that has been provided for one purpose is then used for another reason, unbeknownst to the consumer. Financial institutions, Internet companies health providers and marketers have been caught crossing that line. Meanwhile, identity theft is at an all time high.

Sound and comprehensive privacy laws will help increase consumer trust and confidence in the marketplace and also serve to level the playing field. These laws do not have to ban the collection and use of personal data, merely give the consumer control over their own information.

Consumers should have the right to be fully and meaningfully informed about an institution's practices. Consumers should be able to choose to say "no" to the sharing or use of their information for purposes other than for what the information was originally provided. Consumers should have access to the information collected about them and be given a reasonable opportunity to correct it if it is wrong. In addition to full notice, access, and control, a strong enforcement provision is needed to ensure that privacy protections are provided.

S. 2201 provides the privacy protections consumers deserve.

The CHAIRMAN. Very good. Ms. Lawler.

STATEMENT OF BARBARA LAWLER, CHIEF PRIVACY OFFICER, HEWLETT–PACKARD COMPANY

Ms. LAWLER. Good morning, Mr. Chairman, Members of the Committee. I thank you for the invitation to appear today to discuss the need for stronger Federal protections for consumer privacy and comment specifically on S. 2201.

My name is Barbara Lawler, and as the privacy manager for HP I have global responsibility for HP's privacy policy management, implementation, compliance, education, and communication, both for offline and online approaches. We want to commend you, Mr. Chairman, and the Ranking Minority Member, Senator McCain, and the other Members of the Committee for your commitment to finding solutions to address consumer concerns about protecting their privacy.

3 years ago, when HP first advocated the need for a Federal initiative on privacy, we were virtually alone as a corporation in advocating this position. We think times have changed, and that many more companies and associations will support reasonable baseline Federal legislation for protecting consumers' privacy. It is time to develop national privacy standards.

Let me start by briefly giving you an overall picture of how we manage privacy at HP. We apply a universal global privacy policy built on the fair information practices mentioned today by the Committee, notice, choice, accuracy and access, security, and oversight. In any language the core commitments are the same, with minimal localization required to reflect local country laws. Some key provisions in our policy include no selling of customer data, no sharing of our customer data outside HP without that customer's permission, customer access to core contact data, and a customer feedback mechanism. We insist, through contractual obligations, that suppliers must abide by our policies.

On January 29 of 2001, HP became the first high tech company to self-certify with the U.S. Department of Commerce a safe harbor. This demonstrates our continued leadership to strong privacy practices in the U.S., and because HP manages to a global privacy policy, citizens in the U.S. enjoy the same benefits as those in the EU and elsewhere from HP's privacy policy.

I would now like to turn to the language of S. 2201. First of all, let me say that we are pleased to see that the bill bases its notice and consent requirements on clear and conspicuous disclosure. HP has always felt that informed choice depends upon consumers having available the information they need to make informed choices about with whom they wish to share their personal information.

We are pleased that section 102 recognizes the importance of requiring this basic consumer protection. We are also pleased that there is a place in this legislation for privacy-enhancing technologies like P3P that enhance the notice and choice capabilities for consumers.

We are also pleased that the legislation does not take an either-or stance with regard to the opt-in, opt-out debate. We believe that the continued free flow of nonsensitive personal data with the resulting economic benefits for both consumers and businesses may be best served by an opt-out requirement, allowing room for competitive differentiation. For personal information that is sensitive, an opt-in requirement will give consumers greater confidence in participating in online transactions. HP believes a very constructive discussion can be held as to where the demarcation should be made between opt-in and opt-out.

We also agree on the importance of giving consumers reasonable data access to evaluate the accuracy of information collected. An observation that we would make is that from our experience, data access can be a very complex process. Many companies have multiple data bases that collect data from a number of sources and mediums, and they may not be interoperable.

An integral problem related to this is that of authentication. Confirming that somebody is indeed who they say they are when they request data access could lead into security and identity theft issues. Creating a potential security breach or identity theft problem while trying to address data access is a very real concern.

As to enforcement, we are pleased that the legislation recognizes the importance of the role of the FTC, and we also agree that there is a role for the State Attorneys General in the enforcement of this legislation, and we concur with the balance achieved in the bill be-

tween the rights of States to protect their citizens and the right of the FTC, as the expert agency, to interpret its rules.

One suggestion we would like to make is to find a role for self-regulatory privacy seal programs that have standards equal to or above those required under this legislation. The more eyes and ears available to resolve privacy disputes will benefit consumers, allowing the FTC to certify reputable seal programs to take a first crack at resolving disputes.

Moving to ramp up and comment on the areas where we do have concerns, we must state our strong opposition to the concept of the private right of action for a privacy violation. We agree with the legislation that there is a need for strong, bright lines as to what businesses must do to protect consumer privacy. As we have said, we welcome a healthy debate on opt-in and opt-out, and FTC and State AG enforcement. We would urge the Committee to consider adding language that would allow reputable seal programs to help in protecting consumer privacy. All these initiatives add clarity and certainty to the job of businesses protecting consumer privacy.

We are concerned that a private right of action will create less certainty and clarity in the marketplace as each court will supply its own definition of what constitutes actual harm or reasonable access or reasonable security. Calibrating actual monetary loss from privacy evaluations could become an art rather than a science, as in each case each court, each plaintiff lawyer having their own view.

In other issues addressed in the bill, we believe that there must be a recognition that the offline world and the online world should be subject to the same privacy rules. We would be pleased to work with the Committee on addressing that need for convergence, recognizing the differences in offline and online implementation.

I want to thank you, Mr. Chairman, for the opportunity to testify on S. 2201. HP looks forward to working with the Committee in developing and passing practicable consumer privacy protection this Congress. I would be pleased to answer any questions you may have.

[The prepared statement of Ms. Lawler follows:]

PREPARED STATEMENT OF BARBARA LAWLER, CHIEF PRIVACY OFFICER, HEWLETT-PACKARD COMPANY

Mr. Chairman, Members of the Committee, I thank you for the invitation to appear today to discuss the need for stronger federal protections for consumer privacy, and comment specifically on S. 2201.

My name is Barbara Lawler, and as the HP Privacy Manager, I have global responsibility for Hewlett-Packard's privacy policy management, implementation, compliance, education and communication, in both the online and offline worlds.

By way of background, HP is a leading provider of computing and imaging solutions and services. As a company we are focused on making technology and its benefits accessible to individuals and businesses through networked appliances, beneficial e-services and an "always on" Internet infrastructure.

As a high-tech company that sells to the consumer market, we are deeply committed to strong privacy practices. HP believes that self-regulation *with* credible third-party enforcement—such as the Better Business Bureau privacy seal program—is the single most important step that businesses can take to ensure that consumers' privacy will be respected and protected online. We have also felt for some time, that there must be a 'floor' of uniform consumer privacy protections which *all* companies must adhere to. HP has testified on a number of occasions before Congress about our support for strong, practicable, federal privacy protections. We at HP have had much experience in developing and managing consumer-friendly

privacy policies and practices, so we welcome the opportunity to share our experiences with the Committee about what we think works—and what may not work—in crafting privacy standards.

We want to commend you, Mr. Chairman, the ranking minority Member (Senator McCain), and the other Members of the Committee for your commitment to finding solutions to address consumer concerns about protecting their privacy. Three years ago, when HP first advocated the need for a federal initiative on privacy, we were virtually alone as a corporation in advocating that position. We think times have changed, and that many more companies and associations will support reasonable, baseline federal legislation for protecting consumers' privacy. It is time—past time—to develop national privacy standards. We welcome your leadership in working through the difficult issues that must be resolved if we are to see privacy legislation enacted this year, and we welcome your bill, Mr. Chairman, as a starting point for those discussions.

Let me start by giving you an overall picture of how we manage privacy at Hewlett-Packard. HP applies a universal, global privacy policy built on the fair information practices: notice, choice, accuracy & access, security and oversight. Whether in English, French or Japanese, the core commitments are the same, with minimal localization required to reflect local country laws. Key elements of our policy include no selling of customer data, no sharing of customer data outside HP without customer permission, customer access to core contact data and a customer feedback mechanism. We insist through contractual obligations that suppliers must abide by our policy. Our consumer business requires opt-in for email contact and our B2B business is moving to opt-in as well.

The HP policy can be viewed in its online form at the lower left-hand corner of every hp.com web page: *http://www.welcome.hp.com/country/us/eng/privacy.htm*

The guiding principles for managing data privacy at HP are:

- customers control their own personal data
- give customers choices that enhance trust and therefore enhance the business
- put the customer in the lead to determine how HP may use information about them; and
- have the highest integrity in practices, responses and partners

HP people apply the privacy policy to marketing, support, e-services and product generation using a set of HP-developed tools called the "Privacy Rulebook" and the "Web Site Data and Privacy Practices Self-Assessment Tool".

A sample of current HP global privacy initiatives include:

- company-wide training on implementing privacy standards
- new application development and business rules for company-wide multiple customer database consolidation
- Platform for Privacy Preferences (P3P) implementation for our most active web sites
- Supplier contract compliance assessments

I want to underscore some important distinctions around the 'opt-in' discussion and add some clarity. It's HP policy to never sell or share our customer data without their express permission. HP has many business relationships with other companies. Companies that act as service providers or suppliers to HP are contractually required through a Confidential Non-Disclosure Agreement and Personal Data Protection Agreement to abide by HP's privacy policy.

HP's strategic partnerships and co-marketing partners comprise a different class of business relationships. It is these relationships to which the HP opt-in policy requirement described above applies.

Applying the opt-in standard for marketing contact within HP is an order of magnitude more difficult, but we're committed because it's the right thing to do for our customers. Implementing opt-in for marketing contact requires us to evaluate all customer databases and customer privacy choice data elements, re-engineer the data structures, systems and associated processes, change the privacy question format itself, develop implementation guides and tools, and communicate the new standard HP-wide. Some of the challenges we face are in the areas of managing a program-specific customer privacy choice with a 'topdown' HP request and resolving a large volume of data where the privacy choice is unknown.

On January 29th, 2001, HP became the first high-tech company to certify with the U.S. Department of Commerce for Safe Harbor. This demonstrates our continued leadership to strong privacy practices in the U.S. The Safe Harbor framework offers consistency and continuity for business operations conducted between HP

sites located in the United States and the European Union; this is critical for a global enterprise. And because HP manages a global privacy policy, citizens in the U.S. enjoy the same benefits as those in the EU and elsewhere.

Finally, I would like to put the privacy issue into the larger perspective of consumer confidence in the global electronic marketplace. While consumers are concerned about their privacy online, they are also concerned about whether their credit cards are safe online, and whether if they order a blue vase from a website in Paris or Tokyo, they will get what they order in the quality and condition they expected. In order for online businesses to truly earn the trust of consumers, we need to expand ongoing efforts to make sure that the global electronic marketplace is a clean, well-lighted venue for both consumers and businesses. For example, consumers need to have confidence that when they do business across national borders, there will be a redress system in place should anything go wrong with the transaction.

HP is working with 70+ businesses from around the world through the Global Business Dialogue for electronic commerce to develop a consensus on worldwide standards on consumer redress systems, that is of Alternative Dispute Resolution (ADR). In this effort, we are working with consumer groups and the FTC and the European Commission so that consumers and businesses will be able to quickly, fairly and efficiently resolve complaints related to online transactions.

I would now like to turn to the language of S. 2201.

First of all, we are pleased that the bill bases its "Notice and Consent" requirements upon "clear and conspicuous" disclosure. HP has always felt that informed choice depends upon consumers having available the material information they need to make an informed choice with whom they wish to share their personal information. "Clear and conspicuous" is a term of art used by the FTC to provide robust notification, and we are pleased that Section 102 recognizes the importance of requiring this basic consumer protection. We are also pleased that there is a place in the legislation for privacy enhancing technologies such as P3P, which enhance notice and support capabilities for consumers.

We are also pleased that the legislation does not take an 'either-or' stance on the opt-in, opt-out debate. We think the continued free flow of non-sensitive data, with the resulting economic benefits for both consumers and businesses, will be best served by an opt-out requirement and allowing room for competitive differentiation. For personally identifiable information that is of a sensitive nature (as defined by S. 2201), an opt-in requirement will most likely give consumers greater confidence in participating in online transactions. HP believes a very constructive discussion can be held as to where the demarcation should be made between opt-in and opt-out.

We agree that as a general rule, the consent or denial of a consumer for permission to collect or disclose personally identifiable information should remain in effect until the consumer decides to change their preference.

We also agree on the importance of giving consumers reasonable data access to evaluate the accuracy of information collected. An observation we would make is that from our experience, data access can be a complex process. Many companies have multiple databases that collect data from a number of sources and mediums, and which may not be interoperable. Merging these data files is a prolonged, expensive process, though a process that is underway throughout industry.

A commensurate problem is that of authentication. Ensuring that someone is indeed who they say they are when they request access may bleed into security and identity theft issues. Creating a security breech or an identity theft problem while trying to address the access issue is a real concern.

Having said that, we would like to work with the Committee to find practicable, secure and cost-effective, solutions to the problems of access.

As to enforcement, we are pleased that the legislation recognizes the importance of the role of the FTC. Utilizing clear statutory parameters, we welcome an FTC rulemaking that will allow an opportunity to develop implementation rules and to help define with greater specificity the terms of the legislation. We also agree that there is a role for the state Attorneys General in the enforcement of this legislation, and we concur with the balance achieved in the bill, between the rights of states to protect their citizens, and the right of the FTC—as the expert agency—to interpret its rule.

One suggestion we would make, is to find a role for self-regulatory privacy seal programs that have standards equal or above those required under this legislation. As we have stated, we belong to the BBB privacy program, which we believe is quite strict, and which requires that any consumer complaint must be addressed through a dispute resolution process. The more eyes and ears available to resolve privacy

disputes will benefit consumers, and allowing the FTC to certify reputable seal programs to take a first crack at resolving disputes would be beneficial.

Turning to areas of the bill where we have concerns, we must state our strong opposition to the concept of a private right of action for a privacy violation. We agree with the legislation that there need to be strong, bright lines as to what businesses must do to protect their customers' privacy. As we have said, we welcome a healthy debate on opt-in and opt-out; we welcome FTC and state Attorneys General enforcement, and we would urge the Committee to consider adding language that will allow reputable seal programs to help in protecting consumer privacy. All of these initiatives add clarity and certainty to the job of protecting consumer privacy. We are concerned that a private right of action will create *less* certainty and clarity in the marketplace, as each court will supply its own definition as to what constitutes "actual harm" or "reasonable access" or "reasonable security". Calibrating "actual monetary loss" from privacy violations will therefore be an art rather than a science, as on each case, each court, and each plaintiff lawyer having their own view of the matter.

Consumers deserve adequate protections, and this bill—as we have described—fills a void in privacy protections. At the same time, businesses need certainty as to the rules of the road, so that they can meet the obligations required to address privacy issues. A private right of action in this dynamic environment places this need for clarity and certainty on its head; legislation with a private right of action will offer consumers and businesses less certainty at a time when we need more clarity as to what should be the national, uniform privacy compact.

On other issues addressed in the bill, we believe that there must be a recognition that the offline world and online world should be subject to the same privacy rules. We would be pleased to work with the Committee in addressing that need for convergence recognizing the differences in offline and online implementation.

We also believe that "Whistleblower" law should be uniform across industries and therefore not considered for inclusion in this bill. Industry should not be piecemealed by variations in employment law relating to whistleblowers. And again,—for the reasons stated above—we are concerned about a private right of action included in the Whistleblower section.

Thank you Mr. Chairman for the opportunity to testify on S. 2201. HP looks forward to working with the Committee in developing—and passing—practicable consumer privacy protection, this Congress. I would be pleased to answer any questions that you may have.

The CHAIRMAN. Thank you very much. Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman, Members of the Committee. My name is Marc Rotenberg. I am executive director of the Electronic Privacy Information Center, and I would like to thank you for the opportunity to be here this morning. We have worked with a wide range of privacy and consumer organizations over the years since your original bill was introduced to seek support for important privacy legislation in the Congress.

I think it is clear that across the country public support for privacy protection is still very high, even with the progress which industry has made over the last several years, and there has been progress, there is still a fundamental lack of trust and confidence in the online marketplace.

Legislation does not solve the problem of privacy protection, but I think it will take a big step forward in establishing the type of trust, confidence, stability, and continuity that allow businesses and consumers to participate in this new electronic environment with confidence that the personal information will be protected. The types of problems which the marketplace simple cannot solve are clear today. You can enter into a relationship with an online business, read a privacy policy, provide your personal information,

and the company then decides to change its privacy policy. What do you do at that point?

You can go online, provide information to a business which perhaps is not so well-run. Eventually, they seek the protection of bankruptcy law, and they take their customer data base and they put it online to the highest bidder.

You can go to a commercial web site, look at a 20-page privacy policy and decide you have got better things to do with your life, click "I agree," and take your risks.

What the legislation does is to try to deal with those types of problems that arise specifically in the online environment and make it difficult for consumers to have the type of confidence and assurance that they need when they type in the names of their children, their credit card numbers, where they live, their spouse's names, and so forth.

Now, as you may know, this version of the bill does not go as far as many privacy and consumer groups would like to go. We believe as a general matter that opt-in is a better approach, because it gives consumers better control. We think preemption raises serious concerns about the ability of States to protect the interest of their own citizens, and there are other areas as well where we think further changes might be necessary, but nonetheless I think this is an important step forward.

Now, in my testimony I draw attention to a few areas that I hope the Committee will consider as you look at the legislation a little bit more closely, and I am going to highlight them now very briefly. I am concerned about the law enforcement exception, which is actually a new issue in the drafting of this bill, simply because it is so broad.

The way privacy laws typically work is to create a presumption against disclosure and then to allow exceptions in such circumstances as a warrant or a court order to allow criminal investigations to go forward, but that exception has to be narrowly crafted to ensure that any person who shows up in a business with a piece of paper saying they work for a Government agency is not able to get every record in the possession of that business, and I think it would be in the interest of both businesses and consumers to try to narrow that exception.

I also think if it were possible to expand the access provision so that people would know a bit more about the information about them that is held by the companies, that would be beneficial. As the bill is currently drafted, consumers will largely know only the information that they provide to the company, which is, frankly, fairly self-evident.

Let me say a couple of words, if I may, about the enforcement provision, because I have read a number of comments in the news stories from folks speaking for industry about this provision that it makes me wonder if they are reading the same bill that I was reading. The bill creates a private right of action, without question, but this is a private right of action that I cannot imagine any good attorney wanting to take a case based upon, and the reasons are very simple.

First of all, it requires a showing of actual harm, which is extremely difficult to do in privacy cases, and the reason that Federal

statutes typically set out a liquidated damages amount of $2,500, or $1,000 or whatever an appropriate amount may be, is because it is hard to show harm when personal information is disclosed.

But the second thing that this bill does is to take out any compensation, any award of attorney's fees or for actual costs incurred that a court would routinely award. In other words, even if you prevail, even if you are able to show actual harm under the private right of action set out in this bill, you are only going to be compensated for the amount of your harm and any costs associated with your litigation will not be recoverable.

Now, I think this is just too high a burden for people who are trying to seek redress where their rights have been lost, and I think you have two solutions. One, you can put back in the type of compensation that you would routinely receive in Federal litigation, which includes reasonable attorney's fees, or you can say, if you want to bring a privacy case, go to small claims court, and this is the approach that was taken in the Telephone Consumer Protection Act, and I think that approach could work as well, but this current approach, contrary to what you may read in the newspapers, is not going to open a floodgate of litigation. At best, you may see a trickle of cases from a few people who have a lot of money and want to pursue a privacy claim.

On the distinction between personally identifiable information and sensitive personally identifiable information, I think the privacy community would generally prefer the broader or the higher standard, which would be treat all information as being sensitive, but I do think the bill strikes a reasonable balance, and I think it strikes a common-sense balance that how we view medical information and financial information is not the same as how we view the lettuce we buy or the paper towels we buy in the grocery store, and maybe it is appropriate to make that distinction which the bill makes here.

The one suggestion I would make in terms of where you might draw that line is to consider that issues related to political belief and intellectual freedom really should fall under the category of sensitive personal information. As the bill is currently drafted, you put religious belief as sensitive, personal information, and you put political party affiliation under that category, but a person's political beliefs which may be reflected in their purchases online I think also should be entitled to similar protection.

The approach to technologies for protecting personal policy is very good, and I think that could be expanded to consider a wide range of solutions that industry may develop and that consumers would favor.

So in conclusion, Mr. Chairman and Members of the Committee, I think this is very important legislation. I think it is timely legislation. I think there are an awful lot of people in the United States that would feel more comfortable going online, using the Internet, making transactions and buying stuff, if they knew that there was some privacy protection in place to help safeguard them.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. Chairman, Members of the Senate Commerce Committee, thank you for the opportunity to testify today on S. 2201, the Online Personal Privacy Act. My name is Marc Rotenberg. I am the Executive Director of the Electronic Privacy Information Center in Washington, DC. EPIC is a public interest research and advocacy organization that focuses on emerging civil liberties issues. I am also the chairman of Privacy International, a human rights organization based in London.

It is clear that the protection of privacy remains one of the top concerns in the United States today. Even with the dramatic events of the past year, Americans continue to make clear in opinion polls, news articles, and everyday conversation that one of the great challenges in our era of hi-tech convenience is to avoid the loss of personal privacy.

Today we get sports scores online, read news stories, send messages to friends and colleagues, participate in discussions, buy books and CDs, shop for home loans, make travel plans, and purchase gifts for our relatives. All of this is made possible because of a new computer network technology that has linked together the inexpensive desktop computers that we have in our homes. The benefits of the Internet are clear, but so too are the risks.

In many respects, this ongoing support for the right of privacy is not surprising. Privacy protection has a long history in the United States. Many countries have simply not afforded their citizens the right to use telephones without eavesdropping, to hold credit reporting firms accountable for inaccurate disclosures that impact a consumer's ability to participate in the marketplace, to find a job, to obtain health insurance, or to buy a home.

New privacy laws have frequently been developed in response to the challenges of new technology. Congress enacted privacy laws for the telephone network, computer databases, cable television, videotape rentals, automated health records, electronic mail, and polygraphs. In each case, it was never the intent to prohibit the technology or to prevent the growth of effective business models. Instead, the purpose was to establish public trust and confidence in the use of new technologies that had the ability to gather a great amount of personal information and, if used improperly, to undermine the right of privacy.

With the Internet, a piecemeal approach has been taken. A law was passed to protect the privacy interests of minor children. The FTC exercised its section 5 authority for a limited number of privacy cases. Some US firms endorsed the Safe Harbor Arrangement, providing at least for their European customers, baseline privacy protection. Many companies also attempted to address public concerns about online privacy through the development of privacy policies, the hiring of privacy officials, and support for third-party accreditation services. Some progress has been made. But serious problems remain.

- Companies post privacy policies, enter into relationships with consumers, collect personal information, and then decide to change their policies.
- Companies create assurances of protection, run into financial troubles, seek protection under bankruptcy law, and then sell their customers' data to the highest bidder.
- Companies post privacy policies that require the help of both an English major and a commercial lawyer to understand, and even then the policies are misleading and contradictory.
- Companies acquire information from customers for one purpose and then turn around and sell it for another without the customer's knowledge and consent.
- And companies avoid the adoption of genuine Privacy Enhancing Technologies that could minimize privacy risk and promote the development of electronic commerce because there is no financial consequence to do otherwise.

In each of these examples, there is no market-based solution. And all of this takes place in an environment where the data-collection practices are far more extensive than in the physical world. In theory consumers could bring suit for breach of contract, but privacy harms are difficult to measure, class action lawsuits have not had much success, and even the FTC has struggled to find a way to apply traditional consumer protection law to the new challenges of online privacy.

The Online Personal Privacy Act seeks to establish trust and confidence in the disclosure of personal information in the online environment. This is central to the growth of electronic commerce and the online marketplace. The Act follows the approach of virtually every modern privacy law in the United States. The Act sets out "Fair Information Practices" for the collection and use of personal information pro-

vided by users of the Internet to those who operate commercial web sites or provide Internet services or online services.

As a general matter, the Online Privacy Protection Act contains the basic elements of an effective privacy law. There are provisions for access and for enforcement. There are security obligations and notice requirements. There are opportunities for enforcement. In many respects the Act also tracks the better practices followed by companies today as well as the Safe Harbor Arrangement that US firms have increasingly followed in their online commercial relations with customers in Europe and other countries.

Law Enforcement Exception

As with many privacy laws, the Act creates a presumption against the disclosure of personal information and then sets out limited circumstances when the information may properly be disclosed. For a privacy law to be effective, it is critical that these exceptions be carefully drafted and as narrow as possible. In my opinion, the exception for disclosure to law enforcement agencies (sec. 103(e)) is too broad. In fact, I could not find another privacy law that would make it so easy for so many public officials to get access to personal information that would be otherwise protected in law.

The problem is the list of entities—"law enforcement, investigatory, national security, regulatory agency, or Department of United States"—coupled with the phrase "in response to a request or demand made under authority granted to that agency or department." That formulation essentially defeats the Fourth Amendment purpose of ensuring that the judiciary plays a role where a lawful search is authorized. I urge you to stay with the standard in other privacy laws that grants authority to a "law enforcement agency" acting on a federal or state warrant, a court order, or a properly executed administrative order. This provides the government with a wide range of opportunity to obtain information in the course of a criminal investigation in a manner that ensures judicial oversight and minimizes the risk of abuse.

Access Provision

The access provision (sec. 105) follows a principle widely recognized in US privacy law and that is the ability of person to see the records held by others. Consumers receive access to credit reports, to medical records, and to cable billing information. Under the Privacy Act they are also able to obtain records of information about them held by federal agencies. But the provision in the Online Personal Privacy Act is narrower than it should be. Consumers generally know what information they have provided to companies. What they do not know is what information the company is providing about them to others. The access provisions should allow consumers to be aware of disclosures to third parties.

Also, the bill rightly ensures that copies of this information will be available at a reasonable fee and that the fee is waived in those cases where the consumer may not be able to pay or where there is fraud. A provision should also be included to provide free access in those cases where the provider or operator receives payment or consideration from a third party for the disclosure of the user's information. This is a principle of fairness and equity that will make companies more respectful of the privacy interests of their customers.

Enforcement

Mr. Chairman, the section on enforcement raises several difficult problems. It rightly seeks to provide several ways to ensure actual implementation of the practices set out in Title I, but it is not clear whether these provisions individually, or taken together, provide an adequate means of protection.

It is likely that the primary means of enforcement will be through the Federal Trade Commission since any violation of the Act will be considered a violation of Section 5 of the FTC Act. However, the FTC Act does not provide any actual relief to affected parties. The FTC will have the authority to enter into a consent decree to prevent the company from engaging in similar acts in the future.

The State Attorneys General retain significant authority to pursue actors that violate Title I but the FTC retains the ability to prevent these matters from going forward. Considering that the bill also preempts the authority of states to enact stronger measures to safeguard the interests of their citizens, this provision represents a significant transfer of authority from the states to Washington, DC.

Structurally, the Act places a great deal of faith on the ability of the FTC to pursue privacy violations. I believe that this can be made to work but it will require extensive public oversight. The critical role of the FTC becomes even clearer when you consider the private right of action created by section 203. Some of the industry lobbyists have claimed that this bill will open a floodgate of litigation. But a fair

reading of the Act reveals that it will be remarkable if there is more than a trickle of cases.

Section 203 is drafted in such a way as to pile high all the hurdles of litigation without any of the benefits. Litigants will be required to establish "actual harm" which is difficult in privacy cases, and the reason that federal law typically provides for liquidated damages. They will be required to go into federal district court when violations have occurred but there will be no payment for a lawyer or costs incurred and very limited opportunity for damages if they prevail. It is hard to imagine who but the most affluent would be able to pursue such a case.

The private right of action provision in this bill is far narrower than any other privacy law with which I am familiar. Typically, a federal privacy law allows a person to recover actual damages not less than a set amount of at least $2,500, punitive damages, reasonable attorney fees and litigation costs, and such other relief as a court may determine. And even with these incentives, privacy cases are infrequent and damages, when they are awarded, are nominal. It takes an extremely determined plaintiff to pursue these cases.

At the very least, the Committee should either allow individual consumers to go into small claims court to seek relief for violations of the Act, as they are able to do currently under the Telephone Consumer Protection Act, or if they must go into federal court, the Act should provide for reasonable attorneys fees, costs, and such other relief as a court may provide. Even with this change, proving actual harm in a privacy case will remain very difficult.

Application to Congress and Federal Agencies

Mr. Chairman, I am pleased to see that Title III of the Act extends baseline privacy standards to federal agencies and to the United States Congress. This sends a clear message that Internet privacy protection should apply to both the public and private sector. Title III should also be made clear that nothing in this Act will alter the obligations set out in the Privacy Act of 1974, which applies to all federal agencies that collect personal information on US citizens whether or not they are providers or operators under the definitions of the Act.

But here again I must point out that, unless the law enforcement access provision in Section 103 is narrowed, any federal agency could defeat the purpose of this Online Personal Privacy Act simply by granting itself the authority to routinely engage in actions that would otherwise violate the provisions set out in Title I. It simply does not make sense to pass a privacy law that seeks to impose privacy obligations on a federal agency and then leaves the agency with the authority, if it so chooses, to remove the obligations.

Definition of Sensitive Personally Identifiable Information

The Act makes an important distinction between Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). The first is generally subject to the opt-out approach, while the second would require opt-in. While many privacy experts, including me, have favored the opt-in rule for all transfers of personal information, I believe the approach set out in the bill can be made to work. It reflects a general recognition that there is a distinction between medical and financial information on the one hand and the type of paper towel or lettuce we buy on the other. It also follows an approach that is increasingly found in Europe and other regions of the world to make clear that a stronger privacy standard should apply to more sensitive personal information. The definition of Sensitive Personally Identifiable Information set out in the Act reflect both a commonsense understanding and the practice that is currently evolving.

The one additional subject area that I hope you will consider adding to the category of Sensitive Personally Identifiable Information is for matters of intellectual freedom and political belief. The United States in particular has a long tradition of seeking to safeguard the records of the books that people borrow in libraries, the video tapes they rent, and the cable programs they watch. In a recent case, a state Supreme Court made clear the high level of privacy associated with records of bookstore customers.

With the Internet in particular, there is a significant risk that a very detailed picture of a person's political beliefs could be easily compiled and distributed with little regard for the right of privacy. I believe that if this were done by government actors it would implicate deeply held First Amendment values and should not be permitted.

Privacy Enhancing Technologies

Efforts to develop tools that will enhance online privacy and could diminish the need for further legislation should certainly be encouraged. The bill proposes P3P as one possible approach. I believe a better research program would focus on gen-

uine Privacy Enhancing Techniques that enable online transactions and commerce, and minimize the risk of privacy loss. Such approaches include techniques for "authentication without identification," which means simply that consumers could engage in verifiable transactions with online merchants without disclosing their actual identities much as they do today in the physical world with cash and credit cards. Other research topics might include techniques for enabling online access that do not create additional security risks, developing methods for consumers to more readily track the subsequent disclosure of their personal information, and ensuring by technical measures that individuals will maintain greater control over the personal information they provide to others.

It is clear that a wide range of approaches will be necessary to safeguard online privacy. Technology has a critical role to play. But the privacy technologies must be designed with the central goal of protecting privacy.

Conclusion

In conclusion, Mr. Chairman and Members of the Committee, the Online Personal Privacy Act is an important step forward in the advancement of privacy law in the United States. It responds to overwhelming public support for stronger privacy protection on the Internet. It seeks to ensure that the right of privacy will carry forward as new commercial opportunities are developed and new technologies emerge. I hope the Committee will take the steps necessary to strengthen the provisions in the bill so as to ensure that the intent of the sponsors is realized in practice.

Thank you again for the opportunity to appear before the Committee today. I would be pleased to answer your questions.

The CHAIRMAN. Thank you very much. Mr. Misener.

STATEMENT OF PAUL MISENER, VICE PRESIDENT OF GLOBAL PUBLIC POLICY, AMAZON.COM

Mr. MISENER. Good morning, Chairman Hollings, Senator McCain, Members of the Committee. My name is Paul Misener. I am Amazon.com's vice president for global public policy. Thank you for inviting me to testify today on S. 2201. We greatly appreciate the time and energy you and your staff have committed to consumer information privacy issues, as well as your continuing willingness to hear Amazon.com's perspectives.

Mr. Chairman, Amazon.com is the Internet's No. 1 retailer, with well over 35 million customers. We have as much experience and as much at stake as any entity on these issues. Although Amazon.com has serious concerns about several aspects of this bill, we look forward on behalf of our customers and company to working with you and your Committee to address all of these issues.

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers and, thus, is important to us. Therefore, Mr. Chairman, we share your goal of providing consumers the personal privacy protections they want, and we already provide, with one understandable exception, the substantive protections that a reasonable interpretation of your bill would require.

Indeed, at Amazon.com we manifest our commitment to privacy by providing our customers notice, choice, including opt-in choice where appropriate, access and security. So why do we do so? Well, the reason is simple. Privacy is important to our customers, and therefore important to Amazon.com. We simply are responding to market forces.

Amazon.com believes S. 2201's most serious shortcoming is that, as drafted, it would not apply equally to online and offline activity. In our view, it makes little sense to treat consumer information collected online differently from the same consumer information col-

lected through offline media such as point-of-sale purchase tracking, warranty registration cards, and magazine subscriptions.

Offline privacy practices differ from online practices in only three relevant respects, and in two of these respects consumers get more privacy protection online than offline. In any case, these differences are not addressed in this bill. Rather, virtually identical practices would be treated differently.

Moreover, online transactions account for only a tiny percentage, as Senator Burns pointed out, just 1 percent of all consumer transactions, and people on the unfortunate side of the digital divide, generally those with less money and education, would receive no protections from an online-only law.

This is not to suggest that an online-only approach never was credible. To the contrary, based on what little was known publicly about both online and offline privacy practices as recently as 2 years ago, one easily could have concluded at the time that online privacy issues deserved discriminatory treatment, especially in order to avoid a potential privacy disaster, but now we know there is little justification for discriminating against online.

Mr. Chairman, Amazon.com gratefully acknowledges that S. 2201 contains two important provisions that would be good for our customers, company, and industry. First, it would confirm our believe that the privacy promises a company makes to consumers must still apply to the private information consumers provide to that company even after ownership of the company or information changes.

Second, it intends to preempt inconsistent or additional State laws. It would be difficult or impossible for nation-wide entities to comply with as many as 50 conflicting laws, and it would be unfair, if not also unconstitutional, to permit the citizens of one State to make the privacy decisions for citizens of another.

Mr. Chairman, we also have identified the following areas of serious concern in S. 2201. Amazon.com will focus its cooperative, constructive efforts on these issues as well as on the online-offline parity point, in an effort to provide you and your commitment as much information as possible.

We are very concerned that section 203, on private rights of action, would give overly aggressive litigants a new tool to extract rents from, quote, good-guy companies with relatively deep pockets. It is clear from the recent privacy sweeps that the most popular and, thus, the most successful web sites already are providing outstanding privacy protections. Unfortunately, however, it will be these, quote, good guys that litigants attack, because these are the entities capable of paying big judgments. Indeed, under the current bill it would be far more lucrative to bring a class action suit to catch a good guy on a technicality than catch a bad guy in an egregious act.

And the threat is astounding. A company could be hit with a judgment of $5,000 per user per violation with a showing of but minimal actual harm and no showing of malfeasance. Because class actions are not precluded, there probably would be a class action alleged for every potential violation, and for a company like ours, with 35 million customers, the implications are staggering.

And worse for consumers, allowing such private rights of action would cause the good guys to make their privacy notices much more legalistic and much less readable just so that they would fare better in a lawsuit. We believe a regulatory body such as FTC, on the other hand, could balance the competing interests of legal precision against simplicity.

Another key concern for us are the access and deletion requirements in section 105. This section seems to require data deletion on demand, which would be extraordinarily expensive and would dramatically hinder our efforts to thwart fraud and consumer identity theft. Indeed, this provision would likely end up making consumer identity theft easier by making criminal activity much harder to trace.

Further, the quote, reasonable security requirements of section 106 are cause for great concern, especially among Amazon.com's engineers. Companies have every possible motivation, including extant tort law, to maintain effective security against hackers. Nonetheless, if there is a security breach, it may be very difficult for a company to argue that, quote, reasonable precautions were taken. With little precedent for guidance, the fact of a breach would make any failed security precautions look unreasonable. In other words, without clarifying language, the security reasonableness standard likely would function as a strict liability standard.

Last, we are very concerned about the vague and sometimes incorrect definitions listed in section 401. What for example is, "robust notice" on a web-enabled cell phone or other small-screen device such as a remote terminal on the kitchen wall, or on the automobile dashboard?

Mr. Chairman, in conclusion, Amazon.com is pro-privacy in response to consumer demand and competition. We already provide our customers notice, choice, access, and security. You have called for these same features in S. 2201, and although we have many concerns with this bill, we appreciate that you recognize, as we do, the importance of consumer privacy.

Our foremost concern with S. 2201 is that it would apply only to some companies and only to 1 percent of consumer transactions. Amazon.com respectfully requests that any privacy legislation that moves forward out of this Committee apply to all transactions, not merely those conducted online. Although Amazon.com welcomes two key components of this bill, we also have serious concerns with several other specific provisions. We look forward to working with you and your Committee to address these issues.

Thank you again for inviting me to testify. I welcome your questions.

[The prepared statement of Mr. Misener follows:]

PREPARED STATEMENT OF PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM

Chairman Hollings, Senator McCain, and Members of the Committee, my name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Thank you for inviting me to testify today on S. 2201, The Online Personal Privacy Act.

Although, as I will describe throughout this testimony, Amazon.com has serious concerns about several aspects of this bill, we greatly appreciate the time and energy you and your staff have committed to consumer information privacy issues, as well as your continuing willingness to hear Amazon.com's perspectives.

Amazon.com also gratefully acknowledges that S. 2201 contains two important provisions that we could support. First, this bill would confirm our belief that the privacy promises a company makes to consumers must still apply to the private information consumers provide to that company, even after ownership of the company or information changes. Second, S. 2201 intends to preempt inconsistent or additional state laws. It would be difficult or impossible for nationwide websites to comply with as many as fifty conflicting laws, and it would be unfair (if not also unconstitutional) to permit the citizens of one state to make the privacy decisions for the citizens of another. Both of these provisions in S. 2201 are welcome and would be good for our customers, company, and industry.

As for our concerns, Mr. Chairman, Amazon.com is the Internet's number one retailer and, therefore, has as much experience (and as much at stake) as any other entity on these issues. On behalf of our customers and company, we look forward to working with you and your Committee to address the concerns we raise in this testimony. I hope that you will welcome our perspectives in the constructive and cooperative spirit in which they are offered.

Privacy at Amazon.com

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers and, thus, is important to us. Indeed, as Amazon.com strives to be Earth's most customer-centric company, we must provide our customers the very best shopping experience, which is a combination of convenience, personalization, privacy, selection, savings, and other features.

Therefore, Mr. Chairman, Amazon.com shares your goal of providing consumers the personal privacy protections they want, and we already provide most of the substantive protections that a reasonable interpretation of your bill would require. At Amazon.com, we manifest our commitment to privacy by providing our customers notice, choice, access, and security. Before I describe these four facets of privacy protection at Amazon.com, please allow me to explain how we use customer information.

Personalization at Amazon.com

In general, Amazon.com uses personally identifiable customer information to personalize the shopping experience at our store. Rather than present an identical storefront to all visitors, our longstanding objective is to provide a unique store to every one of our customers, now totaling well over 35 million people. In this way, our customers may readily find items they seek, and discover other items of interest. If, for example, you buy a Stephen King novel from us, we likely will recommend other thrillers the next time you visit the site.

Amazon.com now inserts, among the now-familiar "tabs" atop our Web pages, a special tab with the customer's name on it. When I visited Amazon.com's site last week, for example, the tabs included Books, Electronics, DVDs, and "Paul's Store." By clicking on the "Paul's Store" tab, Amazon.com introduced me to six smaller stores, including one named, "Your Kitchen and Housewares Store," which featured a Calphalon Commercial Nonstick Collector's Edition 10-Inch International Griddle/Crepe Pan, which I promptly bought.

It was no coincidence, of course, that Amazon.com recommended this crepe pan to me, and that I liked it: using so-called "collaborative filtering" techniques, which compare my past purchases (many of which are cookware items) to anonymous statistics on thousands of other Amazon.com purchases, Amazon.com computers automatically—and correctly—predicted that I would want that crepe pan.

Similar personalization is provided in the traditional Amazon.com recommendations on the home page, in purchase follow-up recommendations, in the "New for You" feature, and in some varieties of email communications. Customers can improve the quality of these recommendations in several ways, including by deleting individual Amazon.com purchases from consideration, and by rating the products they buy at Amazon.com or elsewhere. For example, last year I bought my niece a few CDs from the singer Britney Spears but, because I do not want similar music recommended to me, I have deleted these CDs from the list of items Amazon.com uses to produce my recommendations. In addition, on Amazon.com's site, I can rate a CD that I might have purchased at Wal-Mart, in order to improve the quality of Amazon.com's music recommendations to me.

Obviously, Amazon.com's personalization features directly benefit our customers. And, just as obviously, these features require the collection and use of personally identifiable customer information. The question, then, is how do we protect the privacy of this information?

Privacy Practices at Amazon.com

As I indicated earlier, Amazon.com manifests its privacy commitment by providing notice, choice, access, and security.

Notice. Amazon.com was one of the first online retailers to post a clear and conspicuous privacy *notice*. And in the summer of 2000, we proudly unveiled our updated and enhanced privacy policy by taking the unusual step of sending email notices to all of our customers, then totaling over 20 million people.

Choice. We also provide our customers meaningful privacy *choices*. In some instances, we provide opt-*out* choice, and in other instances, we provide opt-*in* choice. For example, Amazon.com will share a customer's information with a wireless service provider only after that customer makes an opt-*in* choice. We simply are not in the business of selling customer information and, thus, beyond the very narrow circumstances enumerated in our privacy notice, there is no information disclosure without consent.

Access. We are an industry leader in providing our customers *access* to the information we have about them. They may easily view and correct as appropriate their contact information, payment methods, and purchase history. And, with a feature called "The Page You Made," customers even can see part of the "click-stream" record of products they view while browsing Amazon.com's online store.

Security. Finally, Amazon.com vigilantly protects the *security* of our customers' information. Not only have we spent tens of millions of dollars on security infrastructure, we continually work with law enforcement agencies and industry to share security techniques and develop best practices.

It is very important to note that, other than an obligation to live up to pledges made in our privacy notice, there is no legal requirement for Amazon.com to provide our customers the privacy protections that we do.

Market Forces at Work

So why do we provide notice, choice, access, and security? The reason is simple: privacy is important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces.

Indeed, if we don't make our customers comfortable shopping online, they will shop at established brick and mortar retailers, who are our biggest competition. Moreover, online—where it is virtually effortless for consumers to choose among thousands of competitors—the market provides all the discipline necessary. Our customers will shop at other online stores if we fail to provide the privacy protections they demand.

These market realities lead Amazon.com to eschew the term "industry self-regulation." We believe this concept—which often is touted as a substitute for legislation and government regulation—suggests that companies must act altruistically in order to provide consumers the protections they deserve. But this suggestion simply is not true. Companies must provide the privacy protections consumers demand or be forced out of business. Nowhere is this more true than among website-based retailers: a consumer can easily choose among hundreds of retailers without leaving her home. Contrast that with brick and mortar retail, which presents consumers with only a very small number of store choices within a reasonable driving distance.

Moreover, as Amazon.com has consistently stated, and last year testified before this Committee, these market realities also lead us to conclude that there is no inherent need for privacy legislation, at least for typical website-based business-to-consumer commerce. The Federal Trade Commission's annual privacy sweeps (this year conducted by the Progress and Freedom Foundation at the behest of the Commission) confirm that those companies with high levels of privacy protections are the ones that succeed in this robust market. There simply is no market failure for legislators to address; indeed, as just noted, the "online" retail market is inherently more competitive than that of traditional "offline" retail. Put another way, if there is a market failure, it is with *off*line, not online consumer transactions.

Notwithstanding these points on the inherent need for legislation, Mr. Chairman, Amazon.com wants to work cooperatively and constructively with you and your Committee on this issue. For S. 2201, we have one general concern, and several specific concerns, which I will describe momentarily. Let me again say, however, that we greatly appreciate the work you and your staff have put into this bill.

Fairness Among Transactions and Consumers

Before addressing specific provisions of S. 2201, please allow me to comment on what Amazon.com believes to be the bill's most serious shortcoming: As drafted, S. 2201 would require companies to provide various privacy protections, but only for a tiny fraction of consumer transactions. And, S. 2201 would not require companies

to provide any protections for tens of millions of American consumers with relatively low incomes and limited educational backgrounds.

As I previously have testified before this Committee, Amazon.com believes that privacy legislation must apply equally to online and offline activities, including the activities of our offline retail competitors. It makes little sense to treat consumer information collected online differently from the same (or often far more sensitive) consumer information collected through other media, such as offline credit card transactions, mail-in warranty registration cards, point-of-sale purchase tracking, and magazine subscriptions.

Offline Privacy Practices. For example, the offline consumer information collection practices of brick and mortar retailers are described on the website (*http://www.epic.org/privacy/profiling/*) of the Electronic Privacy Information Center (EPIC):

> "Many supermarkets are offering membership cards that grant discounts to consumers. What often goes unmentioned is that these club cards enable the store to create detailed profiles of individuals' consumption habits. These profiles are linked to individually-identifiable information, often with the requirement at enrollment that the consumer show state-issued identification. Since many supermarkets sell more than just food (alcohol, cigarettes, pharmaceuticals, etc.), the companies can collect volumes of information about individuals' habits."
>
> "The danger in this profiling is increased by the fact that supermarkets are not limited by law in sharing the information they collect. A supermarket can sell the information to a health insurance company or to other aggregators in order to make a more complete profile on an individual."
>
> "The risks of profiling based on consumption are often derided by supermarket profilers. They may say that 'no one cares if you like asparagus more than broccoli.' But, that's not the issue. Individuals have different definitions of sensitive information. And the profilers aren't interested in whether you're buying one vegetable over another. They are more likely to want to know whether an individual is buying baby diapers or adult diapers."

My wife and I know about these offline privacy practices firsthand. Our son is nearly five months old. Last month, after buying many packages of baby diapers from Giant Food, where we have a "loyalty card," we received a Giant Food "baby brochure," which essentially is an advertising packet. Clearly, this baby brochure solicitation from Giant came merely as a result of purchasing baby products from Giant stores: Giant's computers compiled information about our buying habits and decided to start sending us baby literature.

To be clear, I don't mind receiving such solicitations nor, I believe, do most Americans. It makes more sense for me to receive baby product ads than the brochures I often receive on lawn care services in spite of the fact that I live in a townhouse. I just mind that S. 2201 would ignore such offline practices, yet regulate the exact same personalization services provided by online entities such as Amazon.com.

Warranty registration cards, as EPIC also points out on its website, are yet another way offline entities collect, enter into electronic databases, and sell personally identifiable information that often is entirely unrelated to the subject of the warranty. Several weeks ago, my wife and I needed to buy a new clothes washer and dryer. The warranty registration cards for these large and potentially dangerous appliances had labels telling us to complete and return the cards in the interest of safety. But, for some reason, they also needed to know our household income and our reading habits! Consumers are essentially asked to either provide private information or be unsafe. Similarly, an earlier purchase of a small, but potentially dangerous, space heater included a warranty registration card (again emphasizing the safety aspects of registration) that asked for my household income, where my family took our last vacation, whether we read the Bible, and whether anyone in the household has prostate problems. Because the private information sought from consumers is clearly unrelated to the product subject to the warranty, and probably unrelated to other products sold by the manufacturers of my washer/dryer and space heater, it is obvious that, under the guise of safety, highly private consumer information is being collected and sold.

Obviously, these offline privacy practices are no less deserving—and often far more deserving—of Congress' attention than online practices. Amazon.com firmly believes that, in fairness to consumers (if not also companies), online and offline privacy practices must be treated equally.

The former and current chairs of the Federal Trade Commission have supported this view. In testimony before this Committee nearly two years ago, on May 25,

2000, then-Chairman Robert Pitofsky, in a colloquy with Senator Kerry, testified that,

> "[I] have increasingly come to the view that the theory of distinguishing online from offline is really rather weak. I was recently influenced by one of our advisory panel people who said, "What is the point of treating warranty information from when a consumer files a warranty card, that is just going to be read into an electronic format by some clerk—Why would you treat that information differently from another?" I found that a very powerful argument. I am also influenced by the fact that we hear through mergers, joint ventures, and otherwise, that online and offline companies are merging their databases. And that's another reason we should think about both."

Current FTC Chairman Timothy Muris, in testimony before the Senate Appropriations Committee on March 19, 2002, said that,

> "Consumers are deeply concerned about the privacy of their personal information, both online and offline. Although privacy concerns have been heightened by the rapid development of the Internet, they are by no means limited to the cyberworld. Consumers can be harmed as much by the thief who steals credit card information from a mailbox or dumpster as by the one who steals that information from a Web site."

And, last October, in a speech to the Privacy 2001 Conference, Chairman Muris specifically addressed the scope of privacy legislation, saying,

> "I am concerned about limiting legislation to online practices. Whatever the potential of the Internet, most observers recognize that information collection today is more widespread offline than online. Legislation limited to online practices perhaps seemed attractive when Internet commerce was expanding almost limitlessly. Today, however, it is increasingly difficult to see why one avenue of commerce should be subject to different rules than another, simply based on the medium in which it is delivered."

Mr. Chairman, parity is necessary in fairness to online companies. It simply would not be equitable to saddle online retailers with requirements that our brick and mortar (or mail or telephone order) competitors do not face, nor would it be fair to mislead consumers by telling them their privacy would be substantially protected by an online-only bill when, in fact, only a tiny fraction of their transactions would be addressed.

Online-Offline Differences. Some people contend, however, that online activities deserve discriminatory treatment under the law because of some inherent differences between online and offline business-to-consumer relations. As described above, there are many obvious similarities. I acknowledge, however, that there are three relevant differences between online and offline. Although one of these differences could lead to online consumers having relatively less privacy, the other two differences actually give online consumers *more* privacy protection than offline consumers.

The one difference that potentially gives online consumers less privacy protection is the availability of so-called "click-stream" information, by which a website operator can observe, for example, what individual visitors see while visiting a website. In the retail context, this means web-based retailers can tell what a customer looks at, not just what he buys.

Amazon.com has turned this technical capability into customer-friendly features by which we better personalize our customers' shopping experience. We do this in two principal ways: First, we automatically display items that take into account a customer's recent shopping. If a customer has been looking at cameras, for example, the site may automatically display for her a camera tripod. Second, in our "The Page You Made" feature, we display, on the side of the screen, links back to some of the items the customer has looked at. Thus, instead of scrolling back through the site (the online equivalent of walking back to the other side of the store), we provide a simple way for a customer to get back to the items she earlier examined. Again, these features rely on the use of "click-stream" information.

But even this ability to see what is shopped but not bought is not entirely unique to online entities. Professor Clarke L. Caywood, in his top-selling marketing and PR textbook, *The Handbook of Strategic Public Relations & Integrated Communications* (McGraw-Hill, 1997), describes the same practice in the brick and mortar world:

> "Marketers at Wal-Mart, a large discount retail chain, for example, spend several days each week in their own stores (and those of the competition) watching consumers shop, questioning them about their purchases, and asking them for

feedback. At the end of each week, they return to their headquarters office and, in conjunction with their colleagues who have also spent time in stores in other locales, they discuss what's on the consumer's mind, what trends they need to watch, and what problems they need to correct. Armed with that information, they can tailor all manner of programs to the immediate needs of customers in a very specific local area."

Importantly, even if Congress considers the "click-stream" difference between online and offline to be crucial enough to warrant discriminatory treatment under the law, no federal bill introduced to date, not even S. 2201, is based upon this particular difference. Rather, S. 2201 and previous online-only bills would apply discriminatory legal treatment to activities that, for all practical purposes, are identical online and offline.

And, if differences between online and offline activities are the key, online transactions, in two important respects, actually protect consumer privacy *better* than offline transactions. One respect is physical characteristics. Those Wal-Mart employees said to follow consumers around stores—and, indeed, any employee of a brick and mortar store, watching from the floor or hidden cameras overhead—can see physical personal characteristics unknown to online retailers. Wal-Mart knows your sex and race; if you are pregnant; how well you dress; and if you have acne.

They also know *where* you are. Indeed, when one of Amazon.com's customers visits our store, we cannot know their location. They may be at home, at the office, with their laptop computer at the airport, on the beach with their wireless PDA, or at an "Internet Café" in Paris. We simply don't know. But, when I use my Mobil credit card, Exxon-Mobil knows exactly where I am, and can track my movements. My physical location at any given time is, I would think, highly sensitive information. And, yet, by my reading of Mobil's privacy policy, Exxon-Mobil would not even allow me to opt-*out* of Mobil using that information internally or sharing it with Mobil's "joint marketing partners." S. 2201 would do nothing to change such offline situations, but would require online retailers to obtain (as Amazon.com already does) opt-*in* approval before transferring sensitive information. Again, if there's a privacy problem somewhere, it's offline.

And, for those who point out that offline consumers can always wear dark sunglasses or pay cash in order to remain anonymous, I note that online consumers have many, much easier ways to remain anonymous. They may easily set their web browser to block cookies or may use anonymizing software tools provided by companies such as Zero-Knowledge Systems. Amazon.com's privacy notice describes how to block cookies and provides link to Zero-Knowledge and other anonymizer companies.

Amazon.com Compliance with a Privacy Bill. At last summer's House Commerce Committee hearing on privacy, one Committee member kindly noted that the companies represented, including Amazon.com, are "the good guys." The implication was that the "bad guys" should be the target of privacy legislation, and that we "good guys" need not fear a reasonable law.

In one sense, this Representative was exactly right. Amazon.com does not fear the *direct* effects of reasonable privacy legislation because, unlike the vast majority of our competition in the brick and mortar world, we already provide notice, meaningful choice, access, and security. Indeed, if truly reasonably interpreted, almost all of the substantive requirements of S. 2201 likely would have little *direct* effect on Amazon.com and its customers. (The most notable exception would be the bill's extraordinarily burdensome access/deletion requirement.) We already are providing the privacy protections at the heart of this bill, including excellent access by customers to their own private information, simply because that is what our customers want.

Offline Compliance with a Privacy Bill. However, in addition to a grave fear of being unfairly exposed to a spate of highly unreasonable lawsuits (which I will discuss in a moment), we fear any law that implicitly allows our offline competitors free rein to continue to be privacy "bad guys," unbeknownst to consumers. Indeed, although we are confident that, if consumers really knew what was happening to their private information in the offline world, instead of being mislead to believe that their privacy is more at risk online, they actually would flock to do business with online "good guys" like Amazon.com. But, with the considerable media hype and misinformation surrounding online privacy issues, and the relative dearth of revelations about offline consumer information privacy practices, we believe it would be very unfair to let our competitors surreptitiously collect, use, or transfer consumers' private information.

Consumers Online and Offline. But most importantly, it would be fundamentally misleading to American consumers to enact a law that applies only to online entities

because, for the foreseeable future, the putative protections of such a law would apply to just a tiny fraction of consumer transactions. Last year, online sales accounted for *only one percent* of all retail trade in the United States. Obviously, any law that addresses only online transactions could not benefit consumers much at all compared to one that equally addresses online and offline activities. Moreover, a law that addresses only online activities would have the perverse effect of failing to provide any benefits to those on the less fortunate side of the digital divide. Indeed, consumers who, because of economic situation, education, or other factors, are not online would receive no benefits from an online-only law.

Prior Online-Only Approaches. This is not to suggest that an online-only approach never was credible. To the contrary, based on what little was known publicly about both online and offline privacy practices as recently as two years ago, one reasonably could have concluded at the time that online privacy issues deserve discriminatory treatment, especially in order to avoid a potential "privacy disaster."

No disaster has occurred, and we believe that facts gathered by this Committee and other bodies reveal that an online privacy disaster is no more likely than an offline privacy disaster. In addition, consumers now better understand that computers are used to record both online and offline transactions. The huge, searchable, and transferable computer databases kept by offline companies are just as much at risk as the information collections of online entities. In any case, the bills introduced to date would do little or nothing to forestall privacy disasters, either online or offline.

Moreover, as elaborated throughout this testimony, discussions over the past few years have shown that there are few meaningful differences between online and offline privacy practices, and that some of these differences actually serve to protect consumer privacy better online. And, finally, as documented in the annual online privacy sweeps conducted by the FTC, *et al.*, starting in 1998, it is clear that online entities have made extraordinary strides to enhance their privacy practices over the past four years. Offline privacy practices certainly have not improved at anywhere near this pace, if at all, over the same period.

In sum, Mr. Chairman, although currently-available facts demonstrate that online practices do not deserve discriminatory treatment, there were good reasons why many people believed only a few years ago that such discrimination was warranted.

Privacy Bill Benefits to Industry. Even if this law would do little or nothing to benefit the vast majority of consumer transactions, it has been suggested, such as in S. 2201's Findings, that an online privacy bill would be good for online companies because the consumer trust it would spawn would lead to additional sales. This belief implies that the online industry, which has *not* sought a bill, either does not know what is best for itself or has a hidden agenda. Speaking for Amazon.com, I can say unequivocally that our agenda since our founding in the mid–1990s, has been to provide our customers the very best shopping experience. We believe, with good reason, that if S. 2201 were enacted, it would dramatically interfere with our ability to serve our customers. Indeed, S. 2201 has been reviewed by key personnel throughout our company and has provoked expressions of grave concern, particularly in the engineering department. These "can-do" engineers and programmers, who have built up our computer system all the way from our CEO's garage to the Fortune 500 in just seven years, seriously question whether we possibly could comply with the technical requirements of this bill. And, even if somehow they could make our systems comply, our engineers fear that many of the bill's provisions would seriously jeopardize our systems' security and anti-fraud efforts.

Questionable Industry Support for an Online-only Bill. It is often said that, even if not a majority, at least some in "industry" support an online-only legislative approach. The relevant question is, which industry? The principal proponents of an online-only law do very little business online with consumers. One of the companies, a hardware manufacturer, does but a fraction of its business online, while its biggest competitor does 100% of its business online. It is not difficult to imagine why the first company might support a burdensome online-only approach. Moreover, this same hardware manufacturer sells business hardware and services to Internet-based companies and, potentially at least, would benefit from a law that would require substantial technical investments by online companies. Lastly, the other major technology firm that supports online-only legislation actually manufactures computer components and makes only a tiny percentage of its sales to consumers, whether online or offline. It is difficult to believe this company knows much more about serving web-based customers than Amazon.com knows about semiconductor dumping practices.

Relative Expediency of an Online-only Bill. Finally, it also has been said that "online" and "Internet" transactions are being singled out because it would be too difficult to craft a law that protects the other 99% of consumer transactions. Although

it is hard to believe that expediency is the reason for the "online-only" focus, it is important to note that other bills have been (or soon will be) introduced in Congress that address both online and offline transactions. And, certainly this Committee has jurisdiction over all channels of commerce. Moreover, passing an online-only law at this point likely would delay passage of an offline bill for many years and, thus, actually would hurt the chances of providing privacy protections for consumers offline. In any case, it certainly would not be 99 times more difficult to craft a law that protects 99 times as many consumer transactions.

Conclusion. For all the foregoing reasons, we firmly believe that any privacy legislation that moves forward out of this Committee should apply to all consumer transactions, not merely the one percent conducted online.

Key Positive Provisions in S. 2201

Mr. Chairman, as noted earlier, we believe that there are at least two key provisions in S. 2201 that we could support. We appreciate the fact that you included these in your bill. They are the following:

- Continuing Promise (Section 102(e)(1)(b)): This explicit confirmation that "the promise runs with the information" is good. Although we believe existing common law and Section 5 of the FTC act already would prevent successor entities from treating information less restrictively than was promised at the time the information was collected, we appreciate and support the enactment of this clarifying language, particularly because it removes potential ambiguity in bankruptcy proceedings.
- Preemption (Preamble Section 4): As noted above, this is a necessary and good provision to ensure equal consumer privacy protections nationwide and to allow nationwide entities to comply (it would be virtually impossible for a nationwide website to comply with conflicting rules from multiple jurisdictions). Even though state laws most likely would fail a constitutional challenge, the expense and uncertainty of litigation could be avoided with this sort of Congressionally adopted ceiling. Given the agreement on the need to preempt inconsistent state laws, we merely need to ensure that this language is adequately clear. (Reviewing courts look for clear congressional intent; ambiguous language favors non-preemption.)

Specific Areas of Concern about S. 2201

Mr. Chairman, we also have identified the following areas of serious concern in S. 2201. Amazon.com will focus its cooperative and constructive efforts on these issues, as well as on the online-offline parity point, in an effort to provide you and your Committee as much information as soon as possible. Our principal concerns are as follows:

Private Rights of Action (Section 203):

- As noted above, we fear giving overly aggressive litigants a new tool to extract rents from "good guy" companies with relatively deep pockets. It is clear from the FTC/PFF sweeps that the most popular and, thus, the most successful, websites already are providing outstanding privacy protections. Unfortunately, however, it will be these "good guys" that litigants attack, because these are the entities capable of paying big judgments. Indeed, under the current bill, it would be far more lucrative to bring a class action suit to catch a "good guy" on a technicality than catch a "bad guy" in an egregious act.
- A company could be hit with a judgment of $5,000 *per user per violation* (with up to a $100,000 kicker for repeated violations) with a showing of but minimal actual harm and showing no malfeasance. Because class actions are not precluded, there probably will be a class action alleged for every potential violation. And, if the alleged violation is a part of a company doing business, there will be gigantic cases.
- Allowing such private rights of action will cause the "good guys" to make their privacy notices much more legalistic—and much less readable to consumers—just so that they would fare better in a lawsuit. Unreadably long privacy statements and fine-print legalese would become the norm. A regulatory body such as the Federal Trade Commission, on the other hand, could balance the competing interests of legal precision and simplicity.
- In addition, the uniformity necessary to run nationwide websites would be destroyed by a host of litigants suing companies all across the country. A single authority, such as the FTC, could provide the nationwide approach that private litigation cannot.

State Actions (Section 204):

- In a highly unusual, if not entirely unprecedented, grant of power, this section would allow state attorneys general to bring class actions on behalf of all their residents, unfairly exposing online entities to politically motivated lawsuits.

Access and Deletion (Section 105):

- Several of the terms in this section, such as "reasonable access," "reasonable opportunity," and "suggest," are ambiguously defined and it is unclear how the ambiguity will be resolved. Is this a matter for the Courts or perhaps a broad FTC rulemaking?
- This section seems to require data deletion, which would dramatically hinder our efforts to limit fraud and thwart consumer identity theft. Indeed, this provision likely would end up making consumer identity theft *easier*, by making criminal activity much harder to trace. Further, just imagine asking a bank, or credit card company, or brick and mortar store, to simply "forget" a transaction conducted with them last month, or last year!
- Our information technology department tells us that the access/deletion requirements would require extraordinary costly technical measures. They also fear that, even if it would be possible to meet these requirements, our security and anti-fraud measures would be compromised.
- Finally, there are very narrow exceptions to law enforcement disclosure. One situation not addressed is where a website operator discovers fraud and wants federal help investigating it. Could we be liable if we report fraud to law enforcement or to the victim of the fraud? And what if the victim files a civil suit? Does the fraudster really have a right to contest that motion?

"Reasonable" Security (Section 106):

- Companies have every possible motivation, including tort law, to maintain effective security against hackers. There is no need for a new statute to require it.
- After a security breach, it may very be difficult to argue that "reasonable" precautions were taken. With little precedent for guidance, the fact of a breach would make any failed security precautions look unreasonable. In other words, without clarifying language, a security "reasonableness" standard likely would function as a strict liability standard. On the other hand, to the extent that security practices of other entities become well known, it also would be a concern if "reasonable" were defined as "what everybody else is doing." This interpretation could make it risky for companies to take innovative approaches to security.
- Any detailed, public investigation of whether a company took reasonable precautions might reveal too much to hackers about what a company does and does not do.

Information Collection (Section 101(a)):

- Even if S. 2201 were not modified to apply to offline entities, this provision could unfairly be read to impose requirements on online entities' use of offline information that is, and would remain, available to offline entities without restriction. Online entities should face no more restrictions on offline information than do offline entities.

Notice and Consent (Section 102):

- "Clear and conspicuous," "affirmative consent," and "robust" all are ambiguous terms, despite the definitions offered in Section 401, particularly with regard to the various technical means for delivering this information. For example, robust notice on a web-enabled telephone—with a very small display—might be very different from robust notice on a wide-screen monitor.
- We are concerned about the general prescriptions on "use" disclosures. How detailed must these disclosures be? If the requirement is for super-detailed specifications, then companies will have to anticipate too many small variations on the general theme of how information is used, instead of focusing on the most important general points. Importantly, if too much information is required, consumers will not be presented readable disclosures. Finally, as for "methods of using," we are concerned that this might require the revelation of potentially sensitive technical information not relevant to consumers, but very relevant and useful to hackers.
- For sensitive information, are "opt-in" (in the title) and "affirmative consent" (in the text) the same thing? There is considerable ambiguity in both of these terms. Would the "initial robust notice" requirement force website operators, every time they collect a little more PII, to go back and give robust notice? Yet

if the visitor just returns, and the operator doesn't collect PII, then no robust notice is required. And, under the construct of this bill, every web page visit, which produces click-stream information, creates PII when it's combined with a user's identity. We fear that repetitive opt-out requirements would be burdensome and annoying to consumers.

Definitions (Section 401):

- This section, in addition to containing many ambiguities, incorrectly defines the term "cookie." Further, the definition of "robust notice" is not clear. What is "actual notice"? Is it subjective? Also, the definition itself contains a "use" ("to use or disclose that information for marketing or other purposes"). Does this mean you have to give Robust Notice, before the collection of PII, but Robust Notice is the same as actual notice that you intend to use for marketing or "other" purposes. Is a website's link to a privacy notice "robust" in this way? And what about "robust notice" on a wireless or other small screen device such as the remote terminal on the kitchen wall or the automobile dashboard?

We have identified these principal concerns with S. 2201, and plan to continue our analysis and dedicate our attention to providing the Committee information on each of these points.

Conclusion

In conclusion, Mr. Chairman, Amazon.com is pro-privacy in response to consumer demand and competition. We already provide our customers notice, choice (including opt-in choice where appropriate), access, and security. You have called for these same features in S. 2201 and, although we have many concerns with this bill, we appreciate that you recognize, as we do, the importance of consumer privacy.

Our foremost concern with S. 2201 is that it would apply only to some companies and only to one percent of consumer retail transactions. For the many reasons articulated in this testimony, Amazon.com respectfully requests that any privacy legislation approved by this Committee apply to all consumer transactions, not merely those conducted online.

In addition, Amazon.com has serious concerns with several specific provisions in the bill. Primary of these are the provisions for nearly unfettered class action litigation; access/deletion obligations that would jeopardize our security and anti-fraud efforts; and technically infeasible security requirements. We look forward to working with you and your Committee to address all of these issues.

Thank you again for inviting me to testify; I look forward to your questions.

The CHAIRMAN. Thank you, sir. Mr. Dugan.

STATEMENT OF JOHN C. DUGAN, PARTNER, COVINGTON & BURLING, ON BEHALF OF THE FINANCIAL SERVICES COORDINATING COUNCIL

Mr. DUGAN. Thank you, Mr. Chairman, Senator Hollings, Senator McCain. I am testifying today on behalf of the Financial Services Coordinating Council, whose members include the American Bankers Association, the American Council of Life Insurers, the American Insurance Association, and the Securities Industry Association. These organizations represent thousands of large and small banks, insurance companies, and securities firms that, taken together, provide financial services to virtually every household in America.

The FSCC is keenly aware of the need to maintain the privacy of personal information. With the enactment of the Gramm-Leach-Bliley Act in 1999, thousands of financial institutions across the country have expended enormous amounts of time, energy, and resources to provide financial institution customers with comprehensive privacy protections.

These mandatory protections include notice of the institution's information that must be clear, conspicuous, and provided annually, opt-out choice regarding the institution's sharing of information with nonaffiliated third parties, security in the form of manda-

tory policies, systems, and controls to ensure that personal information remains confidential, and enforcement of privacy protections via the full panoply of enforcement powers of the agencies that already regulate financial institutions, the Federal bank regulators, the Securities and Exchange Commission, State insurance authorities, and the Federal Trade Commission.

All of these mandatory privacy protections apply equally to financial institution consumers in both the offline and online context. The proposed requirements of S. 2201 would apply to financial institutions on top of this already extensive privacy regime.

As a result, the FSCC strongly opposes S. 2201 for the following five reasons.

First, as I said, financial institution are subject already to the comprehensive privacy regulation that Congress carefully debated and enacted just less than 3 years ago. It would be both unnecessary and costly to subject them to the new and conflicting restrictions included in S. 2201, which would translate into two types of notices to consumers, two types of consent provisions, redundant security requirements, and two distinct types of enforcement regimes. The FSCC believes that financial institutions should be subject to a single privacy regime that applies equally in all contexts, as is the case now.

Second, we believe the bill will thwart the development of e-commerce by, for example, imposing dual and conflicting privacy standards for companies that collect information both offline and online, as Senator McCain indicated before, often from the same customer. S. 2201 would severely impair a company's ability to operate under this clicks and bricks business model. Such a company would be forced to maintain two separate information systems, an offline system subject to any applicable offline privacy regulations, and an online system subject to both those privacy requirements and the requirements contained in S. 2201.

In many cases, as I said, the two systems would apply to personal information collected from the same individual, and such a two-tiered system would be extremely costly and burdensome to manage, and it could cause some companies, especially smaller ones, to avoid online operations altogether.

Third, S. 2201 would have a disproportionate impact on financial institutions, even though financial institutions are already subject to extensive privacy regulation. This is so because the bill regulates so-called sensitive information such as account balance and insurance policy information, much more stringently than nonsensitive information. Sensitive information is subject to the opt-in and class action enforcement, while nonsensitive information is subject only to the opt-out and no private right of action.

For most types of businesses, the increased restrictions and sensitive information present relatively few additional problems, because sensitive information does not constitute the core of their business. That is not the case with financial institutions. There, such information frequently is the business of banks, insurance companies, and securities firms.

For example, an online clothing retailer might want to provide special discount coupons to its best customers, who might be those individuals who purchase more than a certain amount of clothing

each year. The retailer's discount offer would be subject to the bill's opt-out requirement, and a violation of the requirement would not be subject to a private right of action or class action enforcement.

In contrast, a bank might want to give its biggest depositors a discount on unrelated financial services such as an insurance product, or a loan, or an insurance company might want to reward a large life insurance policyholder with a discount on his or her car insurance. In these cases, the discount offers would be subject to the bill's opt-in requirement, and any related violations of the statute would be subject to class action enforcement.

Thus, financial institutions, which are subject to much more comprehensive privacy regulation than other online businesses, are subject to the bill's most onerous restrictions with respect to their core businesses, while less-regulated online providers are not. The FSCC believes this is unfair and unnecessary.

Fourth, the FSCC believes that a number of the bill's provisions are simply far too restrictive, including both the opt-in and the access provision. In addition, the bill includes far too few exceptions to both its opt-in and opt-out requirements to recognize legitimate business-sharing and use practices that are necessary for companies to stay in business and provide customer service, such as sharing information with credit bureaus, securitizing mortgages, and a variety of other practices which I have included in more detail in my written statement.

Moreover, the bill's opt-in and opt-out apply to any unrelated use of information, which would act as a new and unprecedented barrier to businesses communicating and marketing products to their own consumers. We think this restriction is just too broad.

Finally, as others have testified, the FSCC believes that the bill's regulatory approach is unnecessary in view of the increasingly effective self-regulatory efforts of the online industry, including through new technologies.

For all of these reasons, the FSCC opposes S. 2201. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Dugan follows:]

PREPARED STATEMENT OF JOHN C. DUGAN, PARTNER, COVINGTON & BURLING, ON BEHALF OF THE FINANCIAL SERVICES COORDINATING COUNCIL

My name is John Dugan, and I am a partner with the law firm of Covington & Burling. I am testifying today on behalf of the Financial Services Coordinating Council ("FSCC"), whose members include the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry Association. These organizations represent thousands of large and small banks, insurance companies, and securities firms that, taken together, provide financial services to virtually every household in America.

The FSCC appreciates the opportunity to testify before this Committee on S. 2201, the Online Personal Privacy Act. We are keenly aware of the need to maintain the privacy of personal information. With the enactment of the Gramm-Leach-Bliley Act in 1999 (the "GLB Act"), thousands of financial institutions across the country have expended enormous amounts of time, energy, and resources to provide financial institution customers with comprehensive privacy protections. Coupled with the protections mandated by the Fair Credit Reporting Act, these consumers now must be provided—

- *Notice* of the institution's practices regarding information collection, disclosure, and use, which must be clear, conspicuous, and updated each year;
- *Opt-Out Choice* regarding the institution's sharing of information with nonaffiliated third parties, and in certain instances, with affiliates;

- *Security* in the form of mandatory policies, procedures, systems and controls to ensure that personal information remains confidential; and
- *Enforcement* of privacy protections via the full panoply of enforcement powers of the agencies that regulate financial institutions, *i.e.,* the federal bank regulators, the Securities and Exchange Commission, state insurance authorities, and the Federal Trade Commission.

In addition to these protections, customers of financial institutions that handle personal health information receive the extensive privacy protections of federal and state medical privacy laws. All of these mandatory privacy protections apply equally to financial institution consumers in both the offline and online contexts. Taken together, they form perhaps the most comprehensive set of mandatory privacy protections in the country. The proposed requirements of S. 2201 would apply to financial institutions on top of this extensive privacy regime.

The FSCC strongly opposes S. 2201 bill for the following reasons. *First*, financial institutions are subject already to the comprehensive privacy regulation described above, which Congress carefully debated and enacted less than three years ago; it would be both unnecessary and costly to subject them to the new and conflicting restrictions included in S. 2201. *Second*, the bill will thwart the development of e-commerce by, for example, imposing dual and conflicting privacy standards for companies that collect information both online and offline, often from the same customer. *Third*, parts of the bill apply much more restrictively to financial institutions, because of the nature of their business, than they do to other types of companies—even though financial institutions are already subject to extensive privacy regulation. *Fourth*, a number of the bill's provisions are simply far too restrictive. *Finally*, the FSCC believes that the bill's heavy regulatory approach is unnecessary in view of the increasingly effective self-regulatory efforts of the online industry, including through new technologies.

I. Financial Institutions and their Customers Don't Need Yet Another Set of Privacy Rules

S. 2201 seems to be aimed primarily at online businesses and advertisers that are not now subject to mandatory privacy regulation. But the bill sweeps in any business that deals with any consumer via the Internet, which means that privacy-regulated businesses like financial institutions are included as well. Because of the financial institution privacy protections described above, which are already in place and apply in the online context, the FSCC believes that the bill's application to financial institutions is unnecessary.

Just over two years ago, Congress carefully considered the costs and benefits of the privacy-related restrictions that ought to apply to financial institutions and their consumers, which resulted in Title V of the GLB Act. Financial regulators subsequently implemented detailed privacy regulations for the first time, and financial institutions have spent many millions of dollars to build systems to comply and protect customer information. Financial institution customers now enjoy the benefit of those protections, which ought to be given a chance to work.

Moreover, S. 2201 would subject financial institutions to a whole new layer of privacy regulations that would apply at the same time as those imposed by the GLB Act and other financial privacy laws. That would mean two types of notices to customers, two types of consent provisions, redundant security requirements, and two distinct types of enforcement regimes. This is far too burdensome and costly. It could also confuse customers, which in turn would result in conflicting instructions by consumers to their financial institutions (*e.g.,* opt-out in one context, opt-in in another). Financial institutions should be subject to a single privacy regime that applies equally in all contexts.

II. S. 2201 Will Thwart the Development of Electronic Commerce

The Internet is bringing enormous social and economic benefits to its users and to nations around the world. It is empowering individuals to seek, receive, and share information and ideas. It is changing how we educate, shop, spend our time, and transact business. And, perhaps most importantly, it is equalizing access to information, giving everyone with a computer and an Internet connection an opportunity both to acquire and use information more effectively.

Throughout its short history, the Internet has been a virtually regulation-free environment. In the United States, regulations affecting the privacy of information online have been limited to only those necessary to protect our most vulnerable online population—children. Because of this philosophy of regulatory restraint, electronic commerce has thrived. According to a recent U.S. Department of Commerce survey, more than half of Americans are using the Internet and among these Internet users, 39 percent of them are making online purchases.

While the European Union has adopted comprehensive privacy regulations, the United States has avoided such an approach. On numerous occasions, government officials have appropriately voiced concern over problems inherent with applying old legislative paradigms to the constantly changing Internet. These concerns appropriately recognize (1) that market-driven solutions to online problems provide the most effective means to ensure the continued growth of the Internet, and (2) that any governmental regulation should target discrete concerns and be carefully tailored to reach no broader than necessary in order to solve the problem at hand. The Children's Online Privacy Protection Act ("COPPA") and the Electronic Signatures in Globalization Act ("ESIGN") reflect this balanced approach. Both laws are narrowly tailored to target specific online concerns and provide a workable legal framework within which these concerns can be resolved.

S. 2201 is a marked departure from this philosophy of restraint and targeted governmental action. The bill treats information collected online differently than information collected by other means and thereby subjects the vast majority of U.S. companies to two substantially different privacy regimes in the offline and online environments. In practice, this approach will retard the use of online channels, or, at the very least, require a company to adhere to the bill's substantive requirements with respect to all of its information collection activities.

Today, companies like financial institutions frequently operate according to a "clicks and bricks" business model under which customer relationships begin offline and migrate online. Specifically, a company collects personal information about a consumer offline when it begins a relationship with a consumer and then again online when the consumer, on his own or through the prompting of the company, uses the company's services over the Internet. In many cases, the information collected online is exactly the same as that collected offline (i.e., name, address, account number), but in other cases the information may be different. As a result, it is fairly typical that a company has one database that includes both personal information initially collected non-electronically (and subsequently entered into a computer) and similar or different information collected over the Internet.

S. 2201 would severely impair a company's ability to operate under this "clicks and bricks" business model. Such a company would be forced to maintain two separate information systems—an offline system subject to any applicable offline privacy regulations (such as the GLB Act or healthcare privacy rules) and an online system subject to *both* those privacy requirements and the requirements contained in S. 2201. In many cases the two systems would apply to personal information collected from the same individual. Such a two-tiered system would be extremely costly and burdensome to manage. And it could cause some companies, especially smaller ones, to avoid online operations altogether.

III. S. 2201 Will Have a Disproportionate Impact on Financial Institutions

S. 2201 creates two categories of personally identifiable information—"sensitive" and "non-sensitive"—and regulates sensitive information much more stringently than non-sensitive information. The bill requires online operators to obtain *opt-in* consent before they collect, disclose, or otherwise use *sensitive* information, and would use a private right of action and class actions to address violations of such requirements. In contrast, with respect to *non-sensitive* information, the bill requires only *opt-out* consent and establishes no express private right of action for individuals.

For most types of businesses, the increased restrictions on "sensitive" information present relatively few additional problems, because "sensitive information" does not constitute the core of their business. That is not the case with financial institutions. S. 2201 defines "sensitive personally identifiable information" to include "sensitive financial information," and that term includes the amount of income earned or losses suffered by an individual; balance "information" regarding any financial services account; any insurance policy information; and outstanding credit card, debt, or loan obligations. Although such information may be incidental to the operations of many online companies, it frequently is *the* business of banks, insurance companies, and securities firms.

For example, an online clothing retailer might want to provide special discount coupons to its best customers, who might be those individuals who purchased more than a certain amount of clothing each year. The retailer's discount offer would be subject to the bill's opt-out requirement, and a violation of the requirement would not be subject to a private right of action or class action enforcement. In contrast, a bank might want to give its biggest depositors a discount on unrelated financial services such as an insurance product or a loan. Or an insurance company might want to reward a large term-life insurance policyholder with a discount on his or her car insurance. In these cases, the discount offers would be subject to the bill's

opt-*in* requirement, and any related violations of the statute would be subject to (and a target for) class action enforcement.

Thus, financial institutions, which are subject to much more comprehensive privacy regulation than other online businesses, are perversely subject to the bill's most onerous restrictions with respect to their core businesses, while less regulated online providers are not. As discussed below, it would be extremely costly and unfair to target financial institutions with some of the bill's most restrictive provisions, *i.e.,* the opt-in and private right of action, which also have particularly negative effects on financial institutions that handle health information.

A. S. 2201's "opt-in" requirement will effectively prohibit core financial institution practices that benefit consumers.

Financial institutions are well aware of the unique position of responsibility they have regarding an individual's personal information, including health information. The member companies of the trade groups belonging to the FSCC are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that these companies have an obligation to assure individuals of the confidentiality of that information.

However, the FSCC strongly opposes S. 2201's opt-in requirement, especially when it is coupled with the bill's unrelated *use* requirement. That is, unlike the GLB Act, which applies only to *disclosures* of personal information by a financial institution to third parties, S. 2201 also restricts virtually any *use* of personal information by the institution itself, even if the information were not disclosed to others and were used to benefit the customer. This would constitute a new and unnecessary roadblock between all companies and their customers.

The combination of the opt-in and unrelated use restrictions would require financial institutions to contact customers and obtain their prior permission to engage in core business activities involving personal information—which in practice would constitute a *de facto* prohibition on responsible information sharing that benefits consumers. Not even Europe's Privacy Directive, which on paper is one the most stringent privacy regimes, goes this far. Instead, the EU Directive permits entities to follow an opt-out approach with respect to the use and disclosure of financial information.

The FSCC believes that there is a fundamental flaw with the way opt-in requirements work. Such provisions deprive consumers of benefits from information sharing, such as discounts on other types of financial products. In essence, an opt-in creates a "default rule" that stops the free flow of information (which is especially critical to Internet transactions). This in turn makes the provision of financial services more expensive and reduces the products and services that can be offered. Further, consumers rarely exercise opt-in consent of any kind—even those consumers who would want to receive the benefits of information sharing if they knew about them. In contrast, a *meaningful* opt-out gives privacy-sensitive consumers as much choice as an opt-in, but without setting the default rule to deny benefits to consumers who are less privacysensitive.

B. S. 2201's narrow exceptions to the bill's opt-in (and opt-out) will prevent critical information sharing by financial institutions.

Privacy regimes that impose customer consent restrictions on financial institutions nearly always include a range of specific exceptions. These exceptions cover circumstances in which consent is either implied, unnecessary, or would impede a legitimate public policy goal. For example, the Gramm-Leach-Bliley Act and its implementing regulations at both the federal and state level recognize well over 30 such exceptions, which are critically important to financial institutions doing business with their customers. Such "doing business" exceptions, which have never been controversial, permit disclosures that are necessary, for example, to prevent fraud, create credit histories, underwrite insurance, engage in risk management practices, securitize loans, outsource functions to agents, obtain legal advice, etc.

In contrast, S. 2201 includes only four exceptions to the bill's opt-in and opt-out requirements. Section 104's exceptions apply to certain information collection, use, and disclosure practices that are necessary to (1) protect the security or integrity of the website; (2) conduct a transaction, deliver a product, or complete an arrangement for which personal information has been provided; (3) provide other products or services that are "integrally related" to the transaction, service, product, or arrangement for which the consumer provided the information; and (4) to comply with law enforcement or a judicial process.

These provisions, although vague, were clearly crafted to reach services provided in the context of completing online retail sales. Yet financial institutions necessarily do much more with online information than engage in marketing or the other ex-

tremely narrow range of activities covered by the bill's exceptions. The combination of the opt-in and unrelated use provisions could potentially shut down core business use and sharing practices, including sharing information with credit bureaus, securitizing mortgages, running normal credit card operations, and engaging in a range of activities related to insurance underwriting. It is unlikely that these activities would qualify as "necessary to conduct" or "integrally related" to the transaction, service, or product obtained by the consumer. This would have the unintended, negative consequence of disadvantaging, rather than helping, consumers.

C. The private-right-of-action provision will invite abusive class action litigation against financial institutions.

Under the bill's private right of action, *any* showing of actual harm involving sensitive information, however small, will provide a plaintiff with a guaranteed recovery of at least $5,000 per violation. Such a provision is clearly intended to attract class action litigation as an enforcement mechanism. Because financial institutions' core business involves information that the bill deems "sensitive," the bill would make them the new target of choice for the plaintiffs' bar.

This is both unfair and unnecessary. Unlike most online businesses, financial institutions are already heavily regulated, and their regulators have broad powers to punish violations of law—which they do not hesitate to exercise. That is why, in the privacy context, Congress chose not to authorize a private right of action or class actions as a means to enforce the GLB Act's privacy provisions. Instead, enforcement is accomplished through the full panoply of enforcement powers of the relevant financial regulator, *e.g.,* federal banking agencies for banks; the SEC for securities firms; state insurance authorities for insurance companies; and the FTC for non-traditional "financial institutions." This enforcement regime works. The FSCC therefore strongly opposes the creation of a new class action mechanism that, while having little impact on most online businesses, would create a huge and unnecessary new source of litigation cost for financial institutions.

D. The bill will have a disproportionate impact on financial institutions that handle health information.

S. 2201 includes individually identifiable health information within the definition of sensitive information that is subject to the bill's stricter opt-in requirements. This ignores the complex and detailed issues surrounding the protection of health information. Financial institutions, particularly insurance companies, must be able to disclose or otherwise use personally identifiable health information to perform essential, legitimate insurance business functions, such as underwriting and claims evaluations. In addition, insurers must be able to disclose and use personally identifiable health information to perform important business functions that are not necessarily directly related to a particular insurance contract but that are essential to the administration or servicing of *insurance policies generally*, such as, for example, developing and maintaining of computer systems. An opt-in that would jeopardize these uses and disclosures of personally identifiable health information would also jeopardize insurers' ability to serve and fulfill their contractual obligations to existing and prospective customers.

Insurers also must regularly disclose personal health and financial information to: (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers; (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers' conduct in the marketplace; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations that typically require broad access to policyholder information. In addition, insurers need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made *not only* to law enforcement agencies, but also to state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators, who work for the insurer. To the extent that S. 2201's opt-in would limit these disclosures, it would undermine the public policy reason for making them—to protect consumers.

Existing federal and state privacy regimes, including the final Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) promulgated by the Department of Health and Human Services as required by the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104–191), provide fundamental protections to the privacy of health information. Unlike S. 2201, the HIPAA Privacy Rule includes a variety of carefully considered exceptions to its authorization re-

quirement in order to strike a proper balance between the legitimate expectations of consumers concerning the treatment of their information and the ability of insurers and others to use personal health information responsibly. Also, many state laws and regulations, particularly those adopted recently to implement the privacy requirements of the GLB Act, contain sections specifically addressing the confidentiality of health information and specifically providing exceptions to their opt-in requirements applicable to disclosures of health information.

In short, the issue of health information privacy is difficult and complex. It is, at best, unclear how the health provisions of S. 2201 compare and/or integrate with existing laws and what impact this legislation will have on financial institutions. At worst, the combination of the opt-in and class action enforcement could have extremely negative consequences.

IV. Other Concerns with S. 2201

There are a number of other fundamental problems with the provisions of S. 2201 that are not unique to financial institutions.

"Use" Restrictions. The problem with the bill's blanket restriction on unrelated "uses" of information is not limited to sensitive information covered by the opt-in. It also applies to nonsensitive information covered by the opt-out. (A business may not disclose or "otherwise use" information collected online without notice and opt-out.) Among other things, this will impair a business from engaging in generally accepted marketing activities *with its own customers*, and a charity from soliciting contributors for additional contributions. Thus, the FSCC believes the use restriction is both unnecessary and overly broad.

Access. S. 2201 will impose access requirements that will be extremely costly and that will reduce security on the Internet. S. 2201 subjects access requests to a vague reasonableness test and fails to exclude information, such as trade secrets or internal operating procedures, to which consumers should never have access. In addition, S. 2201 fails to recognize that information may not be maintained in centralized databases searchable by customer name. (And privacy advocates have long advocated that businesses should *not* be encouraged to establish such centralized databases because of increased possibilities for obtaining and using too much information about an individual too easily.) Even where databases are highly centralized, the costs of complying with this requirement will far exceed the nominal charges permitted under the bill. S. 2201 also fails to define what it means to "delete" a record in an electronic environment. For example, must all back-up tapes be retrieved from storage and searched for relevant records when a "delete" request is received? What about requests to delete personal information when there is a legal obligation or important business reason to retain such information? The bill does not provide guidance on these important questions.

Financial institutions already provide their customers—often in real time—with access to the personal information of greatest concern to them, *i.e.,* their account balances and transaction statements. In addition, the Fair Credit Reporting Act provides consumers with extensive access and correction rights regarding financial institution information that is used to make very significant decisions about them, *i.e.*, to grant or deny credit or insurance. For these reasons, there is no need to impose an additional and vague access requirement that can be used for "fishing expeditions" to search for violations of the Act—especially when violations can be easily translated into class action litigation.

Security. S. 2201 contains security requirements that duplicate those already established for financial institutions in the GLB Act. Specifically, the GLB Act and its implementing regulations require that each financial institution protect the security and confidentiality of customers' nonpublic personal information and implement a comprehensive security program. The differences between the security provisions of S. 2201 and the GLB Act will lead to unnecessary increased costs to ensure that security procedures meet multiple sets of requirements.

V. S. 2201 Is Unnecessary Because Private Sector Efforts Are Working

Finally, apart from the fact that financial institutions are already subject to comprehensive privacy regulation, the FSCC believes that the private sector has taken and continues to take significant steps to address online privacy concerns. These efforts are particularly well suited for solving privacy-related problems on the Internet. This is so because private sector initiatives generally can respond more quickly than legislative solutions to changing technologies and evolving online business and social practices. In addition, private-sector mechanisms, because they are consumer driven by nature, are more likely to permit users to choose among various solutions based on their individual privacy preferences and thereby avoid the problem of over-

and under-breadth that is unavoidable in government regulation, which typically must be one dimensional in nature.

Recent surveys indicate that the private sector's efforts at self-regulation are working. For example, the *Privacy Online* report released earlier this year by the Progress and Freedom Foundation shows that nearly all of the most popular websites (99%) and the vast majority of randomly sampled websites (80%, up from 64% in 2000) post some form of privacy notice if they collect personally identifiable information. Of those websites collecting personally identifiable information, 71% of randomly sampled sites and 89% of the most popular sites offer consumers some form of choice with respect to disclosing that information internally, and almost all (93% up from 77% last year) of the most popular sites and the majority of randomly sampled sites (65%) offer consumers choice over disclosures to third parties. Finally, the survey showed that websites are increasingly likely to tell consumers that they are taking adequate security measures to protect collected information.

In addition, website operators continue to seek certification under seal programs such as TRUSTe and BBBOnLine. By the end of 2001, TRUSTe had certified more than 2000 websites in a variety of industries (up from roughly 500 websites in 1999) and BBBOnLine has certified more than 760 sites, up from 450 two years ago. The FTC has recognized that such seal programs are an effective method for delivering privacy protections to consumers. In particular, the FTC has endorsed seal programs as a means of complying with the provisions of COPPA—the FTC has created a safe harbor so that websites that comply with, for example, TRUSTe's children's privacy seal, will be deemed to be in compliance with COPPA as well.

In addition to these efforts, technology provides compelling solutions to many online privacy concerns. For example, P3P, a privacy-enhancing technology that enables users to specify a level of privacy protection based on a website's practices for tracking data, is continuing to gain acceptance and prominence as an effective method of protecting consumers' online privacy. Among the most popular websites, 23% have implemented P3P, and Internet Explorer 6 includes the P3P function.

In sum, like the Federal Trade Commission, the FSCC believes that the significant and evolving steps taken by the private sector to address online privacy concerns makes additional governmental regulation unnecessary at this time, including S. 2201.

The CHAIRMAN. Very good. Mr. Dugan, we appreciate the position of the bankers and the insurance industry and the securities group, but all you have to do is go get a loan from the bank and you will see how many requirements that are required, and all the information that is necessary to get that loan.

There is no question—getting right to the point, the Federal Trade Commission for 5 years did as we in this Committee asked. We asked them to bring the industry in, correlate it, have hearings, they had numerous hearings time and again, and I mention this because one of the witnesses would quote just part of what Mr. Pitofsky found, that the Federal Trade Commission after 5 years, 2 years ago—so that means we have been on it sevem years—they recommended congressional action to protect the consumer privacy online.

Otherwise, all the fear and bother about the online-offline comparisons, witness after witness has pointed out the differences. It culminated into the Children's Online Privacy Protection under Senator Bryan some 4 years ago, and it has worked wonderfully well. We have not had all of the Chicken Little, the sky is going to fall if you do not regulate the offline with the online.

Otherwise, with respect to the right of action, I will have to agree with Mr. Rotenberg that there is a virus in this Congress, because we are all opposed to politicians and we do not like lawyers, and anything that refers to our right of action, you would think that we had never had any enforcement, and of course when we refer to the different—like the National Highway Transportation Safety Board, we got into Firestone case, and we found out that in a 5-year pe-

riod 99 million recalls, they were all voluntary on account of the private right of action. Not a one in 5 years of the 99 million did the particular governmental Federal commission direct that there be a recall, so we have had hard experience at this Committee level with respect to it.

And the diversity, Ms. Lawler, that you find that might cause trouble of one jury finding one finding and a different jury in a different section of the country finding differently would be sort of confusing. It was not until the forefathers, they put that in in the Seventh Amendment, the Bill of Rights, the trial by jury, for the very reason that we wanted to respect that diversity.

Senator MCCAIN.

Senator MCCAIN. Thank you, Mr. Chairman. I would like to ask first of all, from all the members of the panel, two questions. How should we treat information collected online and offline that is merged together into one consumer data file, and should all identical types of information, whether collected online or offline, be subject to the same privacy restrictions? We will begin with you, Mr. Torres.

Mr. TORRES. Senator, we would love to see a comprehensive privacy bill passed by this Congress and signed by the President into law. Unfortunately, the way that privacy has been treated in this country has been sector by sector. We have looked at video records, we have looked at cable television viewing habits, we have the FCRA, which protects some of the financial information. Telephone records are also covered.

Gramm-Leach-Bliley, while we do not necessarily agree with the position taken by the industry council about the effectiveness of the law, nonetheless that is the law on the books, so the way we have done information in the past, it has been sector by sector, so it is not surprising that we should treat, or that the concept is out there in this bill that we should treat the online sector as kind of—that we should not treat it at all, because we are concerned about implications in the offline world, and I have got three responses to that, really.

We should treat it differently. It is different. It is a different medium. The way they collect information is different.

Senator MCCAIN. My question is, if it is merged together into one consumer data file.

Mr. TORRES. If it is merged together in one consumer data file, it should go to the stronger protections, perhaps, because it is the companies that choose the way they collect their information in either the online or the offline setting. It is the companies that choose to merge that data together. We should not fault the consumer for what the company does and say we cannot control this company because they choose to make this complicated. I do not have a choice, if I think the IRS laws are too complicated, because I have got a lot of complex financial transactions, to say, whoa, this is too complicated, I should not have to comply with this. It is, I choose to merge this information together.

I have got full faith and confidence in this industry, that can find zillions of ways to slice and dice this information, to use it without telling the consumers what they are doing with it, to try to sell consumers junk products, based upon the information they collect from

consumers, and now they cannot figure out how to provide the consumers notice and opt-out, and I mean, the companies are not prohibited from using this information to serve the client, for what the customer gave them the information to do.

What they are not allowed to do without giving the consumer some level of control is to go out and sell this information.

Senator MCCAIN. Mr. Torres, my time is limited, and we have four other respondents. As much as I appreciate your knowledge and your passion, I thank you.

Ms. LAWLER. Let me comment about merging online and offline data sources by way of HP's actual practices, which are that that is the fact today for us, and particularly when we look at the different types of sources, Mr. Misener from Amazon.com mentioned a few. One he did not mention that is actually the single largest source of our customer data is our call center business, and that would be support call centers, or pre-sales call centers, where someone calls because they have a problem they need fixed or help with, with regard to one of their HP products.

So when we talk about merging data into a single data base, I would actually qualify that and say, with many large, global companies like HP, we are not talking about merged data in a data base. We are talking about several, and our efforts have actually focused on reducing the hundreds into the several into the few. It will be never less than a few, given the vast and broad nature of our customers.

Our perspective is, we treat them the same, when you look at the statements made by the FTC last fall, that the presumption is that the offline policies and practices are the same as those stated in our online privacy statement.

Senator MCCAIN. So then they should be subject to the same privacy restrictions, in your view?

Ms. LAWLER. We would be comfortable with that.

Senator MCCAIN. Mr. Rotenberg.

Mr. ROTENBERG. Senator, I think the obligations for companies operating on the Internet should apply when they marry that data with the offline data that is in their possession on the same customers. I think it is very important—you know, if we learned nothing else from the last 5 years, it is clear that the privacy risks associated with the online world are different from those in the physical world.

Senator MCCAIN. Would you agree also, with the changing technology, that the challenges change as well?

Mr. ROTENBERG. Certainly, Senator, I agree the technology will evolve and the law will evolve. The good thing about this bill is that it follows the general principles that have been used in the past to protect privacy and fair information practices, and those principles which really relate to the collection and use of customer information stay pretty much the same even as the technology changes.

But if I may, sir, make one other point, companies operating on the Internet have the benefit of an enormous opportunity that those in the physical world do not. They can track their customers moving from one web page to another. They can plant cookies. They can use e-mails. Some of this is very effective, and some of

it has helped build companies like Amazon that today has 35 million customers, but I certainly think that privacy obligations carry along with those new, innovative business practices.

Senator MCCAIN. Thank you. Mr. Misener, you do not need me to repeat the question, do you?

Mr. MISENER. No, I do not, thank you, sir.

Senator McCain, the same information ought to be treated the same. The consumer's perspective on this is fairly obvious. Why should they care if their privacy is violated through one medium as opposed to another? It ought to be treated equally. It seems to me there is no reason, no principled reason to treat them any differently, or to treat the information any differently.

We have heard from a couple of the other witnesses that there are true differences between the online Internet medium and other channels of commerce. I would submit to you that there are, and if there are differences that warrant legislation specified or specifically tailored to those differences, that is something we ought to talk about. Unfortunately, the way these bills have gone, including S. 2201, is that they treat the same kind of practices differently. They do not hone in on the differences.

I would submit to you, Senator McCain, that in the offline world retailers know the race and the sex and the personal appearances of their customers. We do not. In the offline world, retailers know where the customers are. They can track them around the country. We cannot. We have no idea where they are physically. Those are two very serious privacy differences that actually favor the online world.

If we want to talk about differences, we ought to legislate about——

Senator MCCAIN. Favor the offline world?

Mr. MISENER. Well, that privacy is better in the online world, and so if there are true differences here, let us talk about the differences and hone in on those, but where the collection methods and the use and the treatment of the information and the information itself are identical, they ought to be treated identically under the law.

Senator MCCAIN. Mr. Dugan.

Mr. DUGAN. Senator, I agree, we cannot see how you can treat the information differently. If you operate in two channels at once for the same customer you could not have two separate checking accounts for one person, for example. We think they should be treated the same. They are treated the same under the Gramm-Leach-Bliley privacy scheme that applies to financial institutions in both the offline and the online context, and we think that is appropriate.

Senator MCCAIN. But they are not under this legislation?

Mr. DUGAN. That is correct.

Senator MCCAIN. Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you. Senator Burns.

Senator BURNS. I would like to ask the panel one question along the same lines as Senator McCain asked. Why is it we hear the clamor for privacy online when much or more is collected offline?

Mr. ROTENBERG. Senator, if I could try to answer this, I think it really is because the data collection practices are different. If you

go into a store—you know, it is interesting, you go into a store and you purchase a product, you can pay by cash, and pay by credit card. There is a very good chance the store has no idea who you are unless you choose to sign up for a catalogue or have something shipped to your home, and the thought that walking down an aisle, or picking up a book, or looking at a product that you might be interested in could somehow be recorded is really the exception rather than the rule.

The online world is very different. We know this. I mean, we know this because of the way the cookies operate, because of the http protocols. It is just much easier to follow people online, so when the list of Prozac people is published, that is the kind of problem that could only happen on the Internet.

Ms. LAWLER. Senator Burns, what I would like to add to that, I think it gets down to the fundamental trust relationship that consumers have with the organizations they do business with, and when you have that personal interaction, or you can choose that personal interaction when you walk into a store, or walk onto the concrete in an auto dealer, that is very different than when you cannot see with whom you are dealing. It is a nameless, faceless entity, so I think the perceived and real standards become higher in individuals' minds when they are dealing with a company that may or may not have a brick-and-mortar presence as well.

Mr. MISENER. If you do not mind, Senator, I would just like to add to that that I think part of it—and you have asked why is there more attention being paid to it. I think part of it is frankly just a carryover from what the novelty of the Internet is that really began five, six, 7 years ago, when people were sitting before a computer and it is a mysterious thing. It is a computer, as opposed to the friendly store, or the friendly cards they fill out, the subscriptions I get.

My wife and I just bought a washer and dryer, and the warranty registration card has labeling all over it saying, for your safety, fill out this and return this for your safety, and these are dangerous devices, and so they want to know for my safety what my household income is and whether or not we read the Bible. It is not scary when you fill out the little card in pencil and mail it in, right?

But the reality is, when that card gets filled out and sent in, it gets entered into a huge computer data base which is shared, and the information is sold wherever, and in this instance it is far more safe to share your information with Amazon.com.

Mr. DUGAN. Senator, my only comment is, from a financial institution's perspective, they do not see much difference. Customers are obviously concerned about privacy, but they see it the same way whether it is online or offline.

Senator BURNS. I would imagine—yes, sir, Mr. Torres.

Mr. TORRES. I was just going to say, I think consumers, when they go online, may venture into different areas that they would not necessarily go to in the offline world. I mean, I have looked up an awful lot of, because of a family situation an awful lot of medical information online. The thought that that is being tracked is rather frightening, whereas I might not necessarily go to a bookstore or to the library and look that up, but it is available to me, and so just where you can go online is quite different.

Senator BURNS. As for the second area of concern, in a meeting with various interest parties around about the bill the Committee is concerned with today, I heard a lot of alarm about the private right of action language. Could you comment on the private right of action section contained in S. 2201? Is it overly broad in scope, or is it too limited? Does anybody want to take a shot at that?

Mr. DUGAN. Sure, I will take a shot. We believe it is far too broad, and because financial institutions deal in sensitive information, it is really aimed at financial institutions, even though we already are subject to privacy protections and enforcement.

Our regulators, for example, bank regulators can impose penalties of $1 million a day for violations of privacy violations of the Gramm-Leach-Bliley Act. We think that is sufficient. It is a system that works. There is no reason to apply a private right of action in that circumstance, and the provision in this bill does, as I think someone was saying before, you have to show some actual harm, it is true, but if you show any bit of actual harm, then it is a minimum $5,000 per customer per violation, and if you have millions of customers, as many companies do, that is an invitation to class action litigation.

Senator BURNS. Let me put a footnote on this, and whether it is too broad or too narrow. Give me your idea on safe harbor.

Mr. ROTENBERG. Mr. Chairman, first of all—I am sorry, Senator Burns, as the Chairman explained, you need some kind of private right of action because otherwise all your chips basically sit on the FTC. I mean, that is the way the bill is structured, and if the FTC does not choose to take action, people who may have been actually aggrieved will have no place to turn, and so that is where this provision comes from.

As I explained in my opening statement, I think it is too narrow. I think it places all the burdens of litigation without any of the benefits, and I cannot imagine any lawyer, unless kind of a big-hearted person wants to do it on a pro bono basis, litigating on the basis of this provision, and so I gave two suggestions.

One is to treat it as other privacy statutes do, which is to give people the opportunity to recover for cause. You can even cap, by the way—I mean, I understand the industry concern. You do not need to have sort of big, open-ended damages. You could have a cap on damages, or go into small claims court.

On safe harbor, I think it can be made to work, but enforcement is key, because you have to understand that is another hurdle, another sort of black hole where, you know, we can lose track of what is actually happening and whether there is enforcement of the good provisions in the bill.

Mr. TORRES. Senator, we would be very skeptical of a safe harbor unless it was properly structured in such a way that it was not such a harsh hurdle to overcome, and also have some kind of teeth to it so that the standards were at least equivalent.

And to the private right of action, it is just—I mean, the thought that—we cannot even get—let me put it this way . I work on a lot of different financial and banking issues. We cannot get the bank regulators to go after predatory lenders. The thought that they would go after a bank to seek a $1 million penalty for a privacy violation, I just do not see that happening.

I mean, we talk a lot about accountability and responsibility. You know, we are about to pass a bankruptcy bill that is going to sock it to consumers, and hold them accountable and responsible. Why can't we ask for that same type of standard of industry? If they are so concerned about privacy, they are so concerned about doing the right thing, and they say that they are, why don't they stand up and say, OK, and the private right of action here, the hurdles are high. If anything, it is narrow, but perhaps it does strike the right balance, because to use it, it has got to be a real bad thing for a consumer to use it, so in a way it is self-limiting, and may be the right approach.

Mr. MISENER. Just very quickly, Senator, there are two competing consumer interests here. Consumer interest one is enforcement. They want to ensure that if there is a law on the books that it is enforceable. If it has no teeth, then it is not useful.

On the other hand, consumers also want clear, readable notice given to them. We have these two competing things. One is, companies will try to protect themselves against lawsuits by making the privacy policy extraordinarily long, detailed, legalistic, unreadable. On the other hand, they want to provide their consumers and their customers something that is useful to them, something that actually they will read and understand. These kinds of things are competing interests that an agency like the FTC could take into account.

Yes, it may not have been entirely, precisely, legally correct, but it was trying to communicate to consumers what they were really doing. A class action attorney will have no such balancing desire. He will focus in on the legal precision only, and not care whether or not it was readable.

Senator BURNS. Ms. Lawler.

Ms. LAWLER. Thank you. With regard to the safe harbor, we think there is an excellent place for that in the overall enforcement scheme, and I would comment in particular on our involvement in the BBB online privacy sale program, which also meets the first line of enforcement requirement for the safe harbor self-certification. We think that takes a good place in that regard.

With regard to the private right of action, some of my concerns would be a little bit on the opposite side of the class action suits, and based on observations we have made very recently in the industry and with some of our colleagues, that you have similar to what is happening with many of the State anti-spam laws, which are the spambulance chasers, where individuals——

Senator BURNS. Do not get started on spam.

[Laughter.]

Ms. LAWLER. In any event, what we see is not attorneys getting involved looking for large, deep pockets, but individuals perhaps turning their own interpretation of the law on its side in an effort merely to gain some additional income.

Senator BURNS. Thank you.

The CHAIRMAN. Senator Wyden.

Senator WYDEN. Thank you, and I thank all of our panel. As you know, millions of the privacy notices that get mailed out today, particularly the ones in Gramm-Leach-Bliley just end up in the trash can. They literally show up at the house and into the trash

they go, and these notices are particularly important, because this is something that empowers consumers, and they get a sense of what it is the companies are collecting about them, and for the life of me I cannot figure out why it is not possible to come up with a short, understandable notice and format, so as to give consumers these basic protections.

I would be curious what would be wrong, in the judgment of this panel, with using something along the lines of what is done for nutritional labeling. This is an effort, it is a requirement, it is done the same way on all food products, consumers grow familiar with it, they know to look for it, it is truly a useful tool, and I have got to think that there is enough ingenuity at this table to come up, working on a bipartisan basis with the Chairman and Senator McCain, to come up with something like this that would be helpful to the public. Maybe we could just start with Mr. Dugan, and I have got a few questions for this panel.

Mr. DUGAN. Senator, you raise a good point. In the Gramm-Leach-Bliley act, financial institutions have been frustrated by the fact that in many cases, although they have gone to tremendous time and expense to prepare the notices, as required by the law and the regulations, that they have been perceived as too complicated and too legalistic, and the problem is exactly what Paul was talking about earlier, that in order to comply with the detailed requirements of the privacy regulations, in order to avoid legal liability, there is a real fear that if you get simpler you can expose yourself.

Nevertheless, in the wake of what happened with the first round of Gramm-Leach-Bliley notices, I think there was a lot of education that occurred both with respect to companies and with respect to agencies. It is why the FTC had a big interagency privacy short notice conference in December. It has prompted an effort by the industry to come up and look at precisely the kinds of short notices that you are talking about, but I have to tell you—and I think that is going to make progress. I think we are going to produce something over time, but I have to tell you that is something that takes some care to do right and do in a way that does not expose you to liability.

It took a long time to come up with a food labeling notice that was acceptable to the parties involved and to the Government. I think it is very much a worthwhile endeavor and very much a good point, and it is something we do need to work on in the privacy context.

Senator WYDEN. Are the rest of you comfortable with looking at the nutritional labeling concept just as a model? Obviously, food is different than technology, but this sector has so much expertise it ought to be possible to do something, other than in effect put all of this mail in the trash can, and that is what is happening today.

Mr. MISENER. Senator, we would certainly be happy to look into that sort of thing. We want to be able to communicate as clearly as possible to our customers. I will say that the clear effect of having a private right of action in a bill like this would be to move it the other direction. It would become less clear, much more complicated, much more legalistic, much longer.

Ms. LAWLER. Let me just add that HP would enjoy very much being a part of this discussion. We actually have some best practices that we could bring to the table that we are currently providing in many of our online places for data collection. There is definitely a balance between providing the right level of specificity so that you do not open yourselves up unnecessarily to legal exposure, but I think the overriding principle is definitely clear, simple, informed notice for consumers, and I think along with that, though, is the importance of real, sincere, earnest consumer education on those standards in the labeling that I think are the fair information practices we are talking about.

Senator WYDEN. Let me turn now to you, Mr. Misener, with respect to industry's position on why it is important to have a law. You all are the No. 1 retailer in this field. I mean, it seems to me that if there is an EXXON VALDEZ of privacy, as I have come to describe it, this just shatters consumer confidence. This makes people stay away from the kinds of initiatives your company is built on.

I do not see how all of these voluntary efforts—and I think they are good, and P3P, for example, is the very good, I do not see how they are going to control the bad apples, and I think that is why it is important to have one sensible Federal initiative in this area, and why we spent a lot of time, as you know, working with you, Senator Burns and I and Chairman Hollings, to try to get it done right, but aren't the stakes enormous if nothing is done here, and some of those bad apples shatter consumer confidence?

Mr. MISENER. Thank you, Senator, and you have been consistent in this position for many years, and we certainly appreciate that. If we thought that it would be in the best interest of our customers and company to have a bill like this adopted, we would be here lobbying for it.

Senator WYDEN. But just talk about the concept. Understand, I am not a sponsor of a bill right now. I am interested in working with the Chairman and people like yourself to get something done that addresses this, so just talk conceptually about what happens if the bad apples——

Mr. MISENER. Conceptually, the bill would do nothing to prevent the next EXXON VALDEZ of privacy, would do nothing to get at the bad actors. It would do everything to expose the good guys to litigation.

The little guys who are potentially the bad actors who are not doing well in the market because they are bad actors will not be the targets of litigation. They do not have any pockets. The litigators will go after the big names. They will go after my company and other household names. We see no additional benefit to our customers, either existing or future customers, in having that ability.

Just to sort of pile on, on top if it, Senator, we have really eschewed the term self-regulation. You will never hear me use that because it implies some sort of altruism on behalf of consumers, that companies are going to regulate themselves out of the goodness of their hearts. The reality is, is that companies will lose business. They will lose their existing customers, they will not gain new customers if they do not have the privacy protections that con-

sumers want, and so this is a market-regulating thing. Just as much as the prices of our products are market regulators, so are the levels of privacy protections we provide.

Senator WYDEN. Well, again, I am open with respect to the details here, and that is why I have not signed on to the legislation, but I will tell you, with respect to the key concepts here like preemption, if there are these horrendous incidents where people's medical records, for example, get out, preemption has gone. Industry will not get something that they feel very strongly about. You will have 50 States off to the races, and the whole matter of preemption will be gone, and so we hope you will work with us so we can get it done right, and that is one of the reasons why I am not a sponsor of the legislation today, and I am anxious to work with all of you on it.

A question for you, if I could, Mr. Torres, on the safe harbor, because again, this goes right to the heart of how we are going to bring together folks in the consumer movement who I have worked with for many years, and people in industry. I think with so many e-commerce companies hurting right now, really struggling, it is understandable why they are nervous about possible exposure under a new privacy statute.

How far are you all willing to go to provide this safe harbor kind of concept so that there is a clear path to certainty and safety for companies that we end up rewarding the self-regulatory efforts that are responsible? How far are you all willing to go in terms of meeting industry halfway on the safe harbor idea?

Mr. TORRES. Well, Senator, considering how far we have come on this legislation, to go a little bit farther and talk about how to structure a safe harbor, we would certainly be open to that as a way of recognizing the efforts of some of the better companies out there who have responded to consumer privacy concerns.

Senator WYDEN. One last question, maybe for either of the industry representatives, and Mr. Rotenberg, maybe we could get you into this one.

With respect to access, this, too, is going to be an important issue if we are going to get a meaningful piece of legislation. Access is what makes consumers feel secure. They know that they can get to this critical information. Where is the common ground between industry and consumers with respect to access rights?

Why don't, Mr. Rotenberg, you and Mr. Misener take this one on?

Mr. ROTENBERG. Thank you, Senator. Actually, having been a customer of Amazon, I can say that in many ways Amazon has been a leader in trying to provide their customers with a very extensive display of the personal information that the company has acquired, and it is an important way to establish trust and confidence for the company to disclose to its customers the information that it has on them.

It is really—without access, we are left only with the notices, which are largely like disclaimers. The problems, I think, arise in other circumstances with companies that have not developed this practice that basically say, as this bill seems to suggest, we will give you the information about you that you have already provided to us, and that is not enough, I think, for most consumers to under-

stand what types of profiles are being built, what kind of data is being linked, what other information is informing the company in its decisionmaking with the consumers, and so it is really over in that category of information that I think there is also an interest of access.

Mr. MISENER. Thank you, Senator. Certainly, access is very important. As Mr. Rotenberg points out, Amazon.com has really attempted to provide it as best as possible. I think perhaps the bigger question here is, given that only 1 percent of consumer transactions are consummated online, what about the other 99 percent, no access at all? Is that the result here?

I would think a question to some consumer groups might be, why fight so hard for this 1 percent and leave aside the other 99?

Senator WYDEN. My time has expired. I would only say to this panel I think you all, and the cross-section of people that the Chairman has at this table, you all may have the clout to kill Federal legislation this year. I think that that would be a big mistake. I think it would be a big mistake because a lot of consumers in this country would get hurt, and I think it would be a huge mistake for industry.

As you know, I am the principal sponsor of the Internet tax freedom bill to promote commerce online. You have these privacy problems, and you undo a lot of what we have achieved with the Internet tax freedom bill, so what I have told the Chairman is, I am going to work very closely with him, because I think it is time to get moving, folks.

I think it is time to get a bill passed, and there are areas such as the one I have talked about with respect to the notice provision where, instead of putting all the stuff in the trash cans of America the way we are doing today, under the various requirements of today, we can do something that is constructive by looking at models like nutritional labeling, and so I hope you will work with all of us. I am going to work with the Chairman and Senator McCain, because I think it is time to get going and pass a law, and I thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator. I enjoyed your observation, because let us assume the bill is killed and nothing happens, do not worry about it, the States are going to legislate.

This crowd—I sort of resent polls, and pollster politicians. For 25 years I never did see one, and now I have got to look at them now, because the people do not pay attention until the very end of the campaign, and so that is where you have got to put your money and your TV, but the bankers are not going to get by, and the insurance companies, and the securities. They are going to legislate for you.

And so the reason we are moving now is because the politicians all up here, as much as they dislike private rights of action and whoopee, let's get all the lawyers and everything else like that, they even see now that this is the No. 1 issue on every poll that every one of these Senators are taking, and that is why we are able to finally move, after 7 years.

I can tell you—and I do not mind putting in a bill for the offline the same as the online. I can tell you, 7 years, that will wait 70 years. That is not going anywhere. I can tell you myself. I used to

represent a 123 chain supermarket, and I can see that notice sticking up in the doorway as you come in about how they are going to use the information about what you are buying and sell it around. That poor store would close in the next week. They would lose all their business. People would be scared.

Everybody is interested in privacy offline, online, offline, online, we all know that, but it has gotten to be such a problem and can be managed and will be managed either by the States or the Federal Government, and we here at the Federal level cannot let the perfect be the enemy of the good. I mean, if we wait around, and continue to wait around, we will never get anything done.

So you folks have brought into focus some real concerns about this particular bill. These have been very valuable presentations here today. The Committee is indebted to you, and we will proceed from this point on. We thank you very, very much.

The Committee will be in recess, subject to the call of the chair.

[Whereupon, at 11:55 a.m., the Committee adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. JOHN F. KERRY, U.S. SENATOR FROM MASSACHUSETTS

Mr. Chairman, thank you for holding this hearing. This is a continuation of a process that began in the previous Congress to develop Internet privacy legislation. We are now very near to a bill that empowers consumers to have confidence in the security of the Internet and will allow the Web to continue to grow as an engine of commerce.

I think we are getting very close to achieving that balance. The Chairman has introduced a bill that I am proud to co-sponsor. It is strongly pro-consumer. Its basic premise is that if consumers give their private information out over the Internet, it should be used only for the reason it was given, unless the consumer decides otherwise.

For the first time, we have legislation that creates two separate tracks for personal information—non-sensitive and sensitive. As I have said before, I believe that consumers have different expectations for privacy with respect to their shopping habits or hobbies than they do their medical information or financial information about their religion or sexual orientation.

And, accordingly, the bill allows operators to collect nonsensitive information unless a user decides he or she does not want to permit such an action. Sensitive information is assumed to be private, unless a user allows the operator or service provider to collect that information.

One of the most important elements of the bill is that it requires operators to provide "clear and conspicuous" notice about the collection of personal information. Many well-known websites already do this, much to their credit. However, many online service providers do not have clear, easy-to-understand privacy policies. I believe that requiring this robust notice is a "must" for any privacy legislation. This bill meets that requirement.

Another critical requirement of privacy legislation met by this bill is that it ensures that web site operators and service providers must meet only one standard of privacy. The bill preempts state laws, so that operators are not faced with the cumbersome responsibility of having 51 different privacy notices and 51 different ways for a user to opt-in or opt-out, depending on their residency.

Finally, let me add that technology has an important role to play in this debate. Obviously, if I believed technology held all the answers to guaranteeing Internet privacy, I would not be supporting the Chairman's bill. However, it can help Internet users feel comfortable browsing, shopping and doing research—be it academic or consumer research. The Platform for Privacy Preferences, which I understand Microsoft has recently made available to its consumers, holds great promise in helping consumers determine what sites they can trust and which they are not comfortable with.

Mr. Chairman, today's hearing represents another step in the long march to enacting sound Internet privacy policy. As we go forward on this bill there will undoubtedly be some changes and some further improvements. I stand ready to work with both you and the witnesses, as well as other interested parties to help in that process.

ASSOCIATION OF NATIONAL ADVERTISERS, INC.
April 25, 2002

Hon. ERNEST F. HOLLINGS,
Chairman,
Commerce, Science, and Transportation Committee,
Washington, DC.

Dear Mr. Chairman:

On behalf of the Association of National Advertisers (ANA), I am writing to submit these comments and questions about S. 2201, the "Online Personal Privacy Act." I would like to request that these comments be included in the official hearing record.

ANA is the advertising industry's oldest trade association and the only group dedicated exclusively to enhancing the ability and protecting the rights of companies to market their products and services on a national and regional basis. Our members are a cross-section of American industry, consisting of manufacturers, retailers and service providers. Representing more than 8,000 separate advertising entities, our member companies market a wide array of products and services to consumers and other businesses. Many of our members are actively engaged in e-commerce.

Privacy protection is a critical issue for both consumers and marketers. The future of the Internet and the future of target marketing, which provides the economic foundation for economic efficiency and support for the marketplace of ideas, all depend on our finding a solution to the legitimate privacy concerns of consumers. Marketers understand that the full potential of the Internet will never be reached unless consumers feel secure in the online environment.

S. 2201 contains some positive features, such as federal preemption of state laws. It is a more sophisticated proposal than earlier legislation, recognizing that all information collected online is not created equal. However, we have several significant concerns about the bill:

(1) ANA strongly opposes the access and security provisions of the bill and the private right of action for consumers. These provisions would expose commercial websites to tremendous potential liability and class action lawsuits, and in our view, are unreasonable.

(2) S. 2201 would attempt to regulate the entire universe of online commercial activity and conflict with numerous privacy laws already on the books.

(3) The bill would impose massive new costs and major new burdens on every business that operates online.

(4) Mandating the use of a sweeping opt-in approach for all sensitive information raises serious First Amendment concerns.

(5) The bill would result in a barrage of notice disclosures that would be counterproductive for consumers and businesses.

ANA does not believe that broad new federal privacy legislation is necessary. No government or combination of governments has the resources to police all of cyberspace effectively. We believe that consumers can be best protected through a combination of existing privacy laws and regulations, privacy enhancing technology, effective self-regulation and the backstop of the FTC's current powers to stop false, deceptive or unfair acts or practices.

The Business Community has Responded to Consumer Concerns

ANA believes that the findings in the bill do not adequately recognize the efforts that the business community has made to protect privacy, or the legal enforceability of those steps.

Almost every major commercial website has adopted and posted privacy policies to tell consumers how they collect and use information. The private sector has developed three major seal programs (BBB*Online*, TRUSTe and CPA Webtrust) to assure consumers that websites are in fact carrying out their online privacy policies. New technologies from "cookie cutters" to P3P, the Platform for Privacy Preferences, are providing consumers with the tools they need to protect their privacy. While more remains to be done, we believe the online community has made substantial progress.

The most recent "privacy sweep" shows continued industry progress. That survey of the most popular websites was released in March by the Progress and Freedom Foundation (PFF) and is available at their website at *www.pff.org.*

The survey was conducted by Ernst & Young, based on the methodology of the most recent FTC survey. The key findings of the survey are: (1) websites are collecting less information; (2) privacy notices are more prevalent, more prominent and more complete; and (3) consumers have more opportunities to choose how personally identifiable information is used. Virtually all of the most popular websites surveyed had privacy notices, while 90% of the random sample of websites posted privacy notices. Self-regulation already has gone a long way and continues to be strengthened every day.

FTC Already has Legal Authority to Enforce Privacy Promises

Last October, FTC Chairman Timothy Muris announced a major new privacy agenda for the Commission, including greatly increased resources, more consumer

outreach and education and new enforcement initiatives. At that time, the Chairman stated that the Commission did not need new legislation to protect consumer privacy. We share the Chairman's conclusion that a more vigorous federal cop on the beat, combined with the various efforts of the private sector, can provide consumers with the best protection of their privacy in our new economy.

Once a company posts a privacy policy, the FTC has jurisdiction to go after the website if it does not live up to the privacy promises made. The FTC has brought a number of enforcement cases based on this authority. Thus, the statement in the findings of S. 2201 that current law provides only "minimal" protections is inaccurate.

The Scope of the Proposed Legislation is Very Broad

As you know, the United States has historically taken a sectoral approach to privacy regulation, adopting specific rules to apply to a specific industry and specific perceived problems. As a result, there are more than ten separate federal regulatory privacy regimes, including the Children's Online Privacy Protection Act, the Cable Communications Policy Act, the Telephone Consumer Protection Act, the Video Privacy Protection Act, the Gramm-Leach-Bliley (GLB) Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act, to name just a few.

S. 2201 would seem to regulate the entire universe of online commercial activity. How would the bill relate to all of the other privacy laws already on the books, such as GLB and the health privacy rules? Would companies in those industries be subject to yet another inconsistent privacy regime?

The answer appears to be yes. Under GLB, financial service firms are not required to get consumer consent through opt-in before sharing information with affiliates and subsidiaries. GLB adopts an opt-out approach for this information and this was one of the most contentious issues in the GLB debate. Yet S. 2201 would require an opt-in approach for any collection, use or transfer of sensitive financial information, whether to affiliates or any other group.

One fundamental question that Congress must address is what is the harm that the legislation is seeking to address. Consumers have a legitimate concern about how health or financial information about them might be used by someone else. Thus we have the GLB and health privacy laws and regulations to address those specific concerns and potential harms.

S. 2201 would regulate every part of the online economy, including information about how many shirts someone orders from a retailer and what color, size and price they were. What is the potential harm that can come to a consumer from the use or transfer of that type of general commercial information? Does that potential harm justify a sweeping new privacy regime that imposes costs and burdens on every business in America that uses the Internet?

ANA believes it is critical to determine how S. 2201 would be harmonized with all the existing federal privacy laws. A major diversified business could easily find itself subject to multiple and conflicting requirements and definitions. Conflicting definitions and standards on when a consumer may opt-out of the transfer of information to another entity would be very confusing to consumers and could have a chilling effect on their willingness to permit information to be shared in the marketplace. As discussed below, there is substantial economic evidence that such a result could impose multibillion dollars of costs on various industry sectors.

ANA Supports Uniform, Federal Enforcement of Privacy Laws

If broad privacy legislation is passed by the Congress, then federal preemption should be a key part of the package. The Internet is the first truly global medium and we must be very careful not to allow Internet privacy regulation to become Balkanized through multiple, inconsistent state laws. Therefore, we support language that clearly preempts state law or regulations on the collection, use or disclosure of personally identifiable information obtained through the Internet.

However, the preemption provision in S. 2201 may not actually go far enough. Many of the other federal privacy laws, such as GLB, allowed states to go beyond federal law and adopt their own state laws. It is not clear that the preemption provision in S. 2201 would have any impact on any of these state laws already on the books.

Access and Security Provisions are Unreasonable

ANA is also concerned about the provisions of the bill that would require that consumers receive access to all information held about them by a company. This could be a very costly process for a major global marketer with multiple divisions and subsidiaries. If a packaged goods company has 40 different websites for each of their branded products, are they treated as separate entities for purposes of the access

requirement? If not, the access provision may require the corporate parent to pull together the disparate information held by various subsidiaries to create a dossier on a consumer. This, in turn, raises new security concerns about the ability of hackers or other unauthorized persons to gain access to this newly created profile.

These issues are very challenging and complex. Several years ago, the FTC created an Advisory Committee on Online Access and Security (ACOAS). After months of serious consideration, neither the FTC nor the advisory committee were able to establish clear standards on how to implement these policies.

Everyone agrees on the concepts of access and security, but these issues are the true Gordian Knot of privacy. Providing consumers with broad access to information, without adequate protections, poses potential severe security risks. Overly stringent security precautions can make access very difficult.

How is the access to be provided? Online or offline? How was the $3 fee for providing a consumer access determined? It seems very low in regard to potential collection costs for companies with multiple subsidiaries or disparate databases. Does the committee have any economic evidence of what the actual costs might be for companies to provide access? Without this type of data, it would be dangerous to impose this type of maximum fee. Furthermore, even if the fee could be justified today, can the Congress really assess what would be reasonable fees into the future? A more flexible approach should be developed.

Not all information is created equal. A consumer may have a greater interest in access to sensitive information that a website has collected. Is giving a consumer access to all general marketing information collected about him so important as to justify the cost and burden to companies to provide this access? Are these costs justified in light of potential increased security risks?

Private Right of Action is Unreasonable

We strongly oppose the provisions of the bill that would provide consumers with a private right of action to sue websites that somehow violate the privacy regime.

By creating a damage award of *at least* $5,000 per plaintiff, the bill would put popular websites at risk for large class action lawsuits. Companies would be forced to spend substantial amounts even to defend frivolous claims.

Under section 203 of the bill, upon a showing of actual harm, a consumer is allowed to recover the GREATER of the actual monetary loss from the violation, or $5,000. Assume you had a group of 1,000 consumers who allege that a website has failed to provide reasonable access to sensitive data and a court determined that the actual monetary loss from the violation was $3 per consumer. Under S. 2201, the total award for this case would not be $3,000 (1,000 consumers X $3 per consumer), but rather would be $5 million (1,000 consumers X $5,000 per consumer). This would essentially be a punitive damages model that would strongly encourage litigation even if any actual harm were minimal.

This potential risk could be devastating for many online companies, which often begin as start-up firms or small family businesses. The risk would be very significant even for major multinational firms.

The Opt-In Requirement is Unworkable

Mandating the use of an opt-in approach for the collection and use of all sensitive PII would add tremendous costs and raises serious First Amendment concerns.

ANA is a member of the Privacy Leadership Initiative (PLI). PLI has carried out a number of economic studies to determine the value of information transfer in our economy and the potential costs of an opt-in regulatory regime. In the financial arena, a number of studies demonstrate multi-billion dollar annual savings from accurate credit reporting and the avoidance of fraud due to the collection of data and data access. In the apparel sales area alone, it was demonstrated that if catalog sellers were unable to use routine data that they collect from customers and obtain third party data, they would have to raise their prices by more than $1.4 billion annually. These studies are available at the PLI website, *www.understandingprivacy.org.*

The PLI studies show that gaining affirmative consent under an opt-in system from consumers is a very difficult and expensive process. For example, US West recently conducted an affirmative consent trial using both call centers and direct mail. Outbound telemarketing calls obtained an opt-in rate of 29% of residential subscribers at a cost of $20.66 per positive response. Direct mail was much less successful, obtaining a positive response rate between 5% and 11% and costing between $29.32 and $34.32 per positive response. US West concluded that opt-in was not a viable approach because it was too difficult, too time intensive and too costly.

Therefore, the cost implications of this legislation could be very substantial.

An opt-in requirement, however, implicates issues that go far beyond cost and economic efficiency. Some courts and legal scholars believe that it raises serious First Amendment issues. In 1999 in *U.S. West v. Federal Communications Commission,* 182 F.3d 1224, the 10th Circuit Court of Appeals held that the government must carry out a careful calculation of costs and benefits associated with burdens on speech imposed by an opt-in rule. In that case, the court struck down an FCC rule that contained an opt-in requirement, concluding that the rule violated the First Amendment.

These First Amendment considerations must be carefully analyzed before a broad opt-in approach is adopted, or the government will not meet the requirements laid out by the Supreme Court for the protection of commercial speech.

Balkanization of Information

S. 2201 treats information collected online differently than information collected by other means, such as by telephone, direct mail or fax. Since many businesses provide services to their customers both online and offline, this will mean that information will have to be identified and handled based on how it was received. This requirement will create major incentives to balkanize information about consumers, which will result in significant increased costs with little added benefit for the consumer.

Merging offline data with online data appears to trigger the massive regulatory regime of this legislation. This could create incentives for inefficient information practices, as companies seek to avoid the massive liability they could face under the private right of action provisions of the legislation.

S. 2201 would create numerous classes of information that are subject to special and differential treatment. This is in addition to the different classes of information established by the privacy provisions of GLB and the Fair Credit Reporting Act. This ever-increasing Balkanization of information databases is both costly and inefficient.

Barrage of Notice Disclosures

S. 2201 requires special notice disclosures that differ from the notice requirements of GLB and other federal privacy laws. It may not be possible to satisfy all of these various notice requirements in a single notice. Further, any resulting notices are likely to be complex and confusing to consumers.

Notice requirements are tied to "material" changes in a company's current practices, rather than to the information provided in a prior notice. Thus, even if a company disclosed a prospective practice in its privacy notice, the company would still need to provide a new notice when it actually changes its policies. This will lead to a barrage of notices as new notices are provided in response to relatively minor changes in information practices.

Section 102(d) of the bill states that a website must provide "robust notice" at its "first collection of non-sensitive personally identifiable information from that user." However, the section then goes on to provide that "a subsequent collection of additional or materially different non-sensitive personally identifiable information from that user shall be treated as a first collection." It thus seems that "robust notice" must be provided at every point where "additional" non-sensitive PII is collected. This would lead to massive and repetitive disclosure regimes proliferated across the Internet and every business sector, regardless of cost effectiveness.

Sweeping Government Regulation Does Not Guarantee Privacy Protection

The adoption of sweeping government regulation is no guarantee that consumer privacy will actually be better protected. Europe offers a good example. Although their privacy laws are generally considered more restrictive and comprehensive than those in this country, a January 2001 study by Consumers International indicated that European sites appear often to be actually less effective in protecting personal privacy than American websites. For example, the study found that despite all the rules, 60 percent of European sites lack a privacy policy; only 9 percent of the European sites ask the consumer for permission to sell information about them. Indeed, the study found that U.S.-based sites tended to set higher standards for privacy policies. *Consumers International, Privacy@net: An International Comparative Study of Consumer Privacy on the Internet,* (January 2001).

In fact, Professor Fred Cate of the University of Indiana School of Law has argued that the more restrictive European privacy laws also have failed to quell consumer fears. Despite wide differences in our legal and regulatory approach, polls on consumer privacy concerns show nearly identical results in the U.S. and Europe. For example, Professor Cate cites a Lou Harris & Associates poll in 1999 that found that U.S. and German consumers surveyed demonstrated virtually identical fears about privacy on the Internet. See: *IBM Multi-National Consumer Privacy Survey* (1999).

Therefore, any claims that broad privacy legislation mirroring the European model will drastically diminish public anxiety about privacy and generate dramatic increases in online commercial activity do not seem to be founded on solid research. Nor can they provide the justification for such comprehensive and restrictive legislation as S. 2201.

Conclusion

Privacy gives rise to very complex issues and no one, in industry or government, has all of the answers. We believe the business community is actively working to address the legitimate privacy concerns of consumers.

The online business community has faced tremendous economic challenges in the last year, as companies continue to try to develop profitable business models. Most of the survivors began as small businesses and start-up firms.

S. 2201 is well intended and there are several improvements over earlier proposals. However, ANA believes this bill would impose tremendous new costs and unreasonable burdens on companies of all sizes, and therefore should be rejected.

We appreciate your sincere concerns about consumer privacy and look forward to continuing to work with you and your staff on these critical issues.

Sincerely,

DANIEL L. JAFFE,
Executive Vice President

○